

RECEIVED
SDNY PRO SE OFFICE
2025 APR 10 AM 11:37

UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF NEW YORK

-----X
YUKOS CAPITAL S.A.R.L., YUKOS
HYDROCARBONS INVESTMENTS LIMITED,
STICHTING ADMINISTRATIEKANTOOR YUKOS
INTERNATIONAL, STICHTING
ADMINISTRATIEKANTOOR FINANCIAL
PERFORMANCE HOLDINGS, LUXTONA LIMITED
and MARC FLEISCHMAN, TRUSTEE OF THE 2015
SECURITY TURST, as successor in interest to the
2004 SECURITY TRUST,

Plaintiffs,

v.

DANIEL FELDMAN,

Defendant
-----X

Civil Action No.: 1:15-cv-04964-LAK
Motion for Relief from Judgment

**FEDERAL RULE OF CIVIL PROCEDURE 60(b)(6)
RELIEF FROM JUDGMENT MOTION**

TABLE OF CONTENTS

TABLE OF AUTHORITIES.....	ii, iii
TABLE OF EXHIBITS.....	iii, iv, v
I. INTRODUCTION.....	1
II. BACKGROUND.....	2
A. Factual Background.....	2
B. Vantage Intelligence Ltd.	6
C. Project Yummy.....	7
D. The Project Yummy Emails.....	9
E. The Invoices	13
F. July 13, 2017 Amended Complaint.....	15
G. Links Between the Yukos Group Companies and Aviram Azari.....	15
H. Fraud Unravels All / Farhad Azima.....	17
I. Procedural Background.....	18
III. LEGAL ANALYSIS.....	18
A. Legal Standard for Relief Under Federal Rule of Civil Procedure 60(b): Reasonable Time.....	19

B. Legal Standard for Relief Under Federal Rule of Civil Procedure 60(b): Considerable Discretion and Extraordinary Circumstances.....	20
C. Balancing of the Harms.....	21
D. Not Relitigating or Seeking a Review of a Trial Court Ruling.....	22
E. Attorney-Client Privilege and Work Product.....	23
IV. CONCLUSION.....	24

TABLE OF AUTHORITIES

CASES, RULES and ARTICLES	Page(s)
Federal Rule of Civil Procedure 60(b), Relief from a Judgment or Order.....	18,19,20,22,23
Federal Rule of Civil Procedure 60(b)(6)	2,19,20,21,22
<i>McMillion v. District of Columbia</i> , 233 F.R.D. 179, 179 n.1 (D.D.C. 2005)....	18
<i>Lepkowski v. U.S. Department of Treasury</i> , 804 F.2d 1310 (D.C. Cir. 1986)	18
Federal Rule of Civil Procedure 60(b)(1-3).....	19
Federal Rule of Civil Procedure 60(c)(1).....	19
<i>Pioneer Investment Services Co. v. Brunswick Associates Ltd. Partnership</i> , 507 U.S. 380 (1993).....	19
<i>Ackermann v. United States</i> , 340 U. S. 193 (1950).....	19,20
<i>Klapprott v. United States</i> , 335 U. S. 601 (1949).....	19,20
<i>M.A.S. v. Mississippi D.H.S.</i> 842 So. 2d 527 (2003).....	19
<i>Pierre v. Bemuth, Lembeke Co.</i> , 20 F.R.D. 116 (S.D.N.Y.1956).....	20
<i>Pierce v. Cook & Co. Inc.</i> , 518 F.2d 720 (10 th Cir. 1995), <u>cert. denied</u> , 423 U.S. 1079 (1976)....	20
<i>Radack v. Norwegian America Line Agency, Inc.</i> , 318 F.2d 538 (2d Cir. 1963).....	20
<i>Gonzalez v. Crosby</i> , 545 U.S. 524 (2005).....	20
<i>Liljeberg v. Health Services Acquisition Corp.</i> , 486 U.S. 847 (1988).....	20
<i>Lyons v. Jefferson Bank & Trust</i> , 994 F.2d 716 (10 th Cir. 1993).....	21
<i>Zimmerman v. Quinn</i> , 744 F.2d 81 (10 th Cir. 1984).....	21

In re Gledhill, 76 F.3d 1070 (10 th Cir. 1996).....	21
United States v. 7108 W. Grand Ave., 15 F.3d 632 (7th Cir. 1994)	22
Carter v. Albert Einstein Medical Center, 804 F.2d 805 (3 rd Cir. 1985).....	22
Servants of the Parcels v. Doe, 204 F.3d 1005(10 th Cir. 2000)	22
Voelkel v. General Motors Corp., 846 F.Supp. 1482 (D.Kan 1994), aff’d, 43 F.3d 1484 (10 Cir. 1994)	22
Van Skiver v. United States, 952 F.2d 1241(10 th Cir. 1991).....	22
<i>Charns v. Brown</i> , 129 N.C. App. 635 (1988).....	23
Hoglen v. James, 38 N.C. App. 728 (1978)	23
Charleston Cap. Corp. v. Love Valley Enters., Inc., 10 N.C. App. 519 (1971)	23
Continental Casualty Co. v. Pogorzelski, 275 Wis. 351 (1957)	23
Bruley v. Garvin, 105 Wis. 625, 81 N.W. 1038 (1900)	23
Jacobi v. Podevels, 23 Wis. 2d 152, 127 N.W.2d 73 (1964)	23
Federal Rule of Evidence 502.....	23
Federal Rule of Civil Procedure 26(b)(3).....	23
Restatement (Third) of the Law Governing Lawyers §68 (Am. Law. Inst. 2000).....	23

EXHIBITS

1. UNITED STATES DISTRICT COURT SOUTHERN DISTRICT OF NEW YORK Verdict Form 15-cv-4964 (LAK).....	1,4,15,17,18
2. UNITED STATES DISTRICT COURT SOUTHERN DISTRICT OF NEW YORK Judgment March 20, 201915-cv-4964 (LAK).....	1
3. Sampling of Emails Between Counsel and Feldman’s Feldman23@gmail.com and Caleb23@aol.com Accounts	1,16,17,23
4. United States Department of Justice Victim Notification Letter to Feldman in relation to Defendant Aviram Azari Case Number 2018R00349.....	1,4

5. July 14, 2022 Email from the Federal Bureau of Investigation New York Cyber Division to Feldman Requesting a Meeting about Aviram Azari Case.....	1
6. November 17, 2023 Article #ExxonKnew Hacking Middleman Gets Nearly 7 Years in Prison.....	2
7. October 11, 2024 Email from the United States Department of Justice to Feldman for the Creation of a USAfx File Exchange Account.....	2,4,8
8. December 17, 2024 Email from AUSA Juliana Murray Notifying Feldman that Additional Documents Have Been Uploaded to USAfx with the List of Documents.....	2,8
9. December 17, 2024 Email from AUSA Juliana Murray with Azari Cover Email for Exhibit 21.....	2,5,8
10. January 14, 2025 Email from AUSA Juliana Murray with Cover Emails for Invoices...	2,7,8,13
11. March 10, 2025 Email from AUSA Juliana Murray with Additional Invoices.....	2,8,13,14,19
12. March 31, 2025 Email from AUSA Juliana Murray Regarding 60(b)(6) Motion.....	2
13. July 7, 2022 Reuters / Bing Email Notifying Feldman of the Hacking.....	3,18,19
14. June 30, 2022 Reuters Article: How Mercenary Hackers Sway Litigation Battles.....	3
15. July 2, 2021 Intel News Article: Main Suspect in Potentially Momentous Hacker-For-Hire Case Seeks Plea Deal in NY.....	3
16. June 10, 2020 The Times of Israel Article: Israeli Held In US For Ties to Massive Hacking-For-Hire Operation.....	3
17. US Attorney's Office S.D.N.Y.'s Azari Sentencing Press Release, November 16, 2023.....	3,4
18. July 11, 2022 Bing Email with List of Hacking Emails to feldman23@gmail.com	4,11
19. July 12, 2022 Satter Email with List of Hacking Emails to caleb23@aol.com	4,11
20. March 3, 2017 New Target Project Yummy Email AZ_00061410.....	4,7,9,15
21. Reuter's List of Hacking Emails Including to dan@mondogoal.com	4,10,11
22. Screenshot of dan@mondogoal.com Inbox AZ_00318533 and USAfx Listing.....	5,8,10,15
23. September 11, 2015 Deed of Deposit.....	5,16,20
24. VantageIntelligence.com Screenshot Martin Parr Biography.....	5,15

25. Excerpt from the Trial Transcript of Martin Parr’s S.D.N.Y. Testimony.....	5,15
26. Steven Theede Deposition Transcript Excerpt June 28, 2016.....	6
27. Male Escort Email from King to Godfrey December 8, 2011.....	6
28. VantageIntelligence.com Screenshot Gretchen King Biography.....	7,9,14
29. VantageIntelligence.com Screenshot Organizational Chart.....	7,8,15,16,20
30. Ninety-Four Azari Phishing Emails Shared via USAfx by the DOJ on October 11, 2024.....	8,9,10,11,12,13,15,16
31. Eleven Nerosia Ltd./Azari Invoices Provided by the DOJ on October 11, 2024.....	8,9,10,14,15
32. Five Documents Shared via USAfx by the US DOJ on December 17, 2024.....	8,9,10,13,14,15
33. Nerosia Ltd./Azari Invoices 108 & 153 to King Provided by the US DOJ on March 10, 2025.....	8,13,14,15
34. Seven Cover Emails For Invoices From Nerosia Ltd. / Azari to King	8,9,14,20
35. March 2015 Notional Holdings / Shvetsova Invoices.....	10,16
36. Excel Spreadsheet of Spear phishing Emails by Date.....	10,15
37. January 29, 2019 Hacking Attempt Spoofing David Rourke of Delphi Management.....	11,16
38. Maltin Litigation Support List of Hacking Emails.....	11,12,16
39. Excerpt from Maltin Litigation Support Hacking Investigation Report June 19, 2024.....	16
40. March 25, 2024 High Court of Justice Decision Farhad Azima.....	17
41. England and Wales High Court (Chancery Division) Decisions: Ras Al Khaimah Investment Authority -and- Farhad Azima [2022] EWHC 2727 (Ch).....	18, 21
42. March 26, 2024 Brick Court Chambers: Judgments in Favour of Emirati Sovereign Wealth Fund Set Aside on Grounds of Fraud by the Fund.....	18

I. INTRODUCTION

The jury trial in the above captioned matter took place over three weeks in March of 2019 before the Hon. Judge Lewis Kaplan. The jury dismissed eight of the ten claims, but found that I had breached my fiduciary duty on the two remaining claims but that I had done no harm. The decision was without a finding of fraud, dismissed the faithless servant claim and thus awarded no damages under that claim or any other. The jury rejected the notion that I had acted disloyally or with evil motive or intent for either found breach by answering no to questions 10(a) and 10(c) of the Verdict Form. [EXHIBIT 1] A nominal fine of \$1.00 per breach was levied. [EXHIBIT 2]

Since the March 2019 verdict, new evidence has come to light that could not have been discovered previously, and demands that the two judgments that are the subject of this motion, reflected on the Verdict Form as claims 1 and 5, [EXHIBIT 1] be set aside with prejudice due to exceptional circumstances. There was an illicit coordinated covert cyber hacking attack on me (and three actual and potential trial witnesses) throughout this litigation, undertaken on behalf of and / or for the benefit of the plaintiffs, which fundamentally undermined the judicial process.

A hacker retained on behalf of the plaintiffs illegally accessed my email accounts throughout the above captioned litigation, which included the email accounts, feldman23@gmail.com and caleb23@aol.com,¹ which were used to communicate with counsel, those with expert witnesses and emails related to draft submissions, [EXHIBIT 3]² thereby breaching the attorney-client privilege and accessing work product created in anticipation of litigation / trial.

The hacking was a deliberately planned and carefully executed scheme, utilizing insider information. A judgment is irrevocably tainted when one party criminally accesses the other party's email communications throughout the litigation, including those with counsel, and that a new trial would not cure the issues arising from this breach. It is incurable behavior that goes far beyond simple skullduggery / what is acceptable in litigation.

The hacking was effectuated by a group that included Aviram Azari ("Azari"), owner of an Israeli intelligence firm and a former Israeli police officer specializing in covert surveillance and accessing of data through spear-fishing.³ The covert nature of Azari's work made it impossible for me to uncover the breach on my own. It was only in July 2022, when a Reuters investigative reporter informed me of the hacking and the subsequent confirmation by the United States Attorney's Office of the Southern District of New York ("US Attorney's Office") in the same month, that I was made aware of what happened. On November 14, 2022, I was added to the United States Department of Justice's ("DOJ") Victim Notification System for Azari's case. [EXHIBIT 4] I have been working with the Federal Bureau of Investigation's New York Cyber Division ("FBI") and US Attorney's Office since July, 2022. [EXHIBIT 5] Their investigation is

¹ I no longer have access to dan@mondogoal.com as the company no longer exists, so I am not able to determine if communication with counsel was also done via this email address.

² Exhibit 3 includes screen shots of the sent box from two of my email accounts evidencing that I used both accounts targeted by the hackers to communicate with counsel. There are hundreds of such email communications. I chose a limited example to include here.

³ Spear phishing is a targeted email attack that uses personalized information to trick specific individuals or organizations into revealing sensitive information, such as login credentials or financial details.

on-going.⁴ Azari was sentenced to eighty (80) months in prison on November 16, 2023. During Azari's sentencing hearing I gave an in-person victim impact statement to the court. [EXHIBIT 6]⁵ Dmitri Merinson ("Merinson"), also a victim of Azari's hacking and a former Yukos Group Companies⁶ ("YGC") colleague of mine who was employed by the plaintiffs for over a decade, who was too intimidated to appear at the March 2019 trial, provided a written victim impact statement added to the record at Azari's sentencing.

On October 11, 2024, the United States Attorney's Office shared with me via their USAfx File Exchange network one hundred eleven (111) documents related to the hacking campaign against me, [EXHIBIT 7] shared another five documents via the File Exchange network on December 12, 2024, [EXHIBIT 8] forwarded one additional document on December 17, 2024, [EXHIBIT 9] sent another seven documents via email on January 14, 2025, [EXHIBIT 10] and two more via an email sent on March 10, 2025. [EXHIBIT 11] Finally, on March 31, 2025, upon review of the present motion, the US Attorney's Office wrote via email that they, "do not see anything from my read through that is factually inaccurate." [EXHIBIT 12]

As a result, this motion is being filed within a reasonable time, as I am faultless for the delay. Prior to the sentencing of Azari, I had not received any evidence from the US Attorney's Office and was not comfortable revealing my cooperation with the government investigation by filing this motion, which would have alerted the plaintiffs that I knew of their nefarious actions. I have continued to receive evidence to support this filing through March 2025. Prior to receiving the one hundred twenty-six (126) documents from the DOJ, I did not feel that I had established via documentary evidence the necessary nexus to the litigation to file this Federal Rule of Civil Procedure 60(b)(6) motion. Now that I testified at Azari's sentencing hearing and I have been be provided with numerous salient evidentiary documents, I am more confident in being able to proceed. I cannot afford to pay lawyers to file this motion, which is a factor in deciding whether the timing of this motion is reasonable as is explained below. As a result, with concern that I do get this filed within a reasonable time, I prepared this motion pro se.

II. BACKGROUND

A. Factual Background

In March 2003, I was appointed Corporate Secretary of Yukos Oil Company ("Yukos"). The company, based in Moscow, Russia, was the fourth largest oil company in the world. Yukos was closely held by six Russian oligarchs, most of whom are Jewish (the relevance of this will be apparent below). Subsequently, the company and the oligarchs fell out of favor with the Russian government, the oligarchs were either imprisoned or fled the country, and Yukos was forced into bankruptcy in August 2006 and ultimately out of business. I continued working for YGC, a network of Yukos subsidiaries outside of Russia working to protect the company's foreign assets.

⁴ The S.D.N.Y. US Attorney's office is currently attempting to extradite Azari's co-conspirator Amit Fortlit from London. Fortlit is also a former Israeli private eye accused of conspiracy to carry out computer hacking.

⁵ Page 4, lines 5-8.

⁶ Yukos Group Companies is an umbrella term, which includes all of the plaintiffs, both individuals and entities, who filed the original suit.

Unfortunately, for reasons not relevant to this motion the relationship with my co-workers deteriorated, and after eleven years my time with Yukos and YGC came to an end in October 2014.

After rejecting a severance package, YGC sued me in 2015 in the United States District Court for the Southern District of New York (“S.D.N.Y.”). In March, 2019, the case was heard before a jury with the Hon. Judge Lewis Kaplan presiding. Among the many wild conspiracy theory claims made by the YGC was that I had worked for their litigation opponents and wiled away money in foreign jurisdictions. Both claims are patently untrue, and were dismissed by the jury. The case was presented over three weeks. I was successful in defending against eight of the ten claims but was found to have breached two fiduciary duties, without causing any harm or there being a finding of fraud. As a result, the Hon. Judge Kaplan imposed a nominal fine of \$1 to be paid for each breach to each plaintiff. The findings were appealed by both sides and although the breaches against two of the plaintiffs were dismissed, the jury’s findings were otherwise left intact as to the other plaintiffs. Plaintiffs’ appeals were dismissed.

On July 7, 2022, more than three years after the judgment, I received an email, from Christopher Bing (“Bing”), a Reuters investigative reporter. [EXHIBIT 13] Bing and his Reuters colleague Raphael Satter (“Satter”) published an article on June 30, 2022, just prior to contacting me entitled, How Mercenary Hackers Sway Litigation Battles.⁷ [EXHIBIT 14] In his email to me, Bing informed me that in at least 2017 and 2018, while preparing for the 2019 trial, I was the victim of an expansive mercenary hacking campaign directed by Azari, a private investigator working on behalf of wealthy clients, typically Jewish Russian oligarchs with ties to Israel. The hacking according to Bing and Satter’s investigation was, “often designed to steal documents or information relevant to different litigation battles around the globe.” [EXHIBIT 14] The private investigator behind the attacks on my three email addresses was adjudicated to be Azari, who served in an Israeli police covert surveillance unit and was a coveted private investigator in Israel. He pled guilty to the hacking and was sentenced to eighty (80) months in federal prison.

Azari’s hacking campaign, referred to as “Dark Basin,”⁸ was part of a sprawling hacking-for-hire operation. [EXHIBIT 15]⁹ The targets were routinely one side of a legal or advocacy issue, or business dispute. [EXHIBIT 16]¹⁰ As recounted in the US Attorney’s Office S.D.N.Y.’s Azari sentencing press release of November 16, 2023:

Clients hired Azari to manage “Projects” that were described as intelligence gathering efforts but were, in fact, hacking campaigns specifically targeting certain groups of victims... [EXHIBIT 17]

Azari pled guilty but refused to cooperate with authorities. However, at his sentencing hearing after I told Azari:

⁷ This article can be found here: <https://www.reuters.com/investigates/special-report/usa-hackers-litigation/>

⁸ Dark Basin was coined by Citizen Lab, a University of Toronto at the Munk School of Global Affairs, that helped uncover Azari’s hacking scheme.

⁹ This article can also be found at: <https://intelnews.org/tag/operation-dark-basin/>

¹⁰ This article can also be found at: <https://www.timesofisrael.com/israeli-held-in-us-for-ties-to-massive-hacking-for-hire-operation/>

You're weak. If you are truly sorry, you should be giving the names of the people who hired you. [EXHIBIT 7] Page 3, lines 5-8.

Azari responded to me directly and said:

I ask forgiveness. Daniel, you don't know everything.¹¹ [EXHIBIT 7] Page 4, Line 24

Upon receiving the July 7, 2022, email from Bing, I contacted the US Attorney's Office and met with two New York based FBI Cyber Division agents and Assistant United States Attorney ("AUSA") Juliana Murray ("Murray"). They confirmed that I am a victim of Azari's hacking. [EXHIBIT 4] I have met, exchanged emails and spoken with the FBI agents and AUSA Murray numerous times. At the AUSA's request, I appeared in-person to provide a victim witness impact statement at Azari's sentencing hearing on November 16, 2023. After the Azari's sentencing upon hearing him tell me that I, "did not know everything" I switched from providing information to the US Attorney's Office to asking for information and it was only post-sentencing that the DOJ was willing to share information.

On July 11, 2022, Bing sent me a list of some of the targeting phishing attempts by Azari to hack into my feldinan23@gmail.com account ("Address One"). [EXHIBIT 18] At least four of them, from 3/16/16 to 3/31/17 are from a spoofed delphi.bm account [EXHIBIT 18]. On July 12, 2022, Bing's colleague Satter sent me a list of six emails sent by Azari to my caleb23@aol.com account ("Address Two"). [Exhibit 19] One of these emails, sent on 3/30/17 was also from a spoofed delphi.bm account. [Exhibit 19] Delphi is a fund management firm overseeing a fund in which I had invested YGC money and was the focus of Claim 5. [EXHIBIT 1] This investment was well known by David Godfrey ("Godfrey") and Steven Theede ("Theede")¹², the two driving forces of the litigation in the S.D.N.Y. against me, as well as lawyers and accountants working for Godfrey, but was not known publicly. The name of the fund management firm is even less well known.

The use of the spoofed Delphi domain and the time period of the hacking coinciding with the time period of the S.D.N.Y. litigation are clear indications that the emails targeting me were sent on behalf of YGC. Azari's use of 'spear phishing' emails sought to maximize the chance of targets opening the emails that would give the hackers access to their emails is widely noted, including in the US Attorney's Office's Azari sentencing press release. [EXHIBIT 17] The only way Azari and the hacking teams at CyberRoot and BellTroX InfoTech Services¹³ ("BellTroX") would know that the use of Delphi would deceive me into opening an email was if someone from YGC informed them of that. Insider knowledge was required. The same goes for the targeting of Address One, Address Two and Address Three. Address One uses my last name, Address Two uses my middle name and Address Three is related to a little-known startup company and uses my first name. Inside knowledge possessed only by those noted above would be required to know to target these email accounts with emails from a fake Delphi address on consecutive days. We know that both Address One and Address Two were sent to a group of hackers to target me on 3/3/2017. [EXHIBIT 20] The third email dan@mondogoal.com ("Address Three") was hacked and targeted starting in 2016 per a list of hacking attempts provided to me by Bing and Satter. [EXHIBIT 21]

¹¹ Exhibit 7, a news article, failed to note that Azari addressed me directly by name with this comment.

¹² Godfrey and Theede are the former General Counsel and CEO of Yukos respectively,

¹³ BellTroX's founder, Sumit Gupta, is wanted by the FBI for his involvement in hack-for-hire operations.

The FBI and the US Attorney's Office recovered a screen shot of my Address Three inbox from Azari and uploaded it to the USAfx fileshare system me as AZ_00318533 [EXHIBIT 22], demonstrating that he had successfully accessed this account. Azari emailed the screen shot to a colleague on 1/18/16, as described by the US Attorney's Office in an email dated 12/17/2024. [EXHIBIT 9]

Azari was routinely hired by Russian oligarchs with ties to Israel. The largest shareholders of Yukos are Leonid Nevzlin, Mikhail Brudno and Vladimir Dubov, all Jewish Russian oligarchs living in Israel. Over one billion dollars has been distributed to these oligarchs by the YGC. YGC is controlled by Theede, Bruce Misamore¹⁴ ("Misamore") and Godfrey, the former CEO, CFO and General Counsel of Yukos respectively and members of the Dutch stichtings¹⁵ that have for years controlled the international assets of Yukos. YGC at the direction of Theede, Misamore and Godfrey often employ business intelligence companies, such as Diligence Inc. ("Diligence"), to gather information on litigation opponents. They hired as an in-house investigator, Gretchen King ("King"), formerly employed by Diligence, to do the same, often employing illegal tactics. YGC, via King, paid for the contents of a laptop stolen from Nikita Tolstikov who worked for litigation opponent Rosneft.¹⁶ Per a Deed of Deposit dated September 11, 2015, [EXHIBIT 23] Misamore stated on September 2, 2015, that YGC stole information from litigation opponents' laptops for use in courts.¹⁷ This is not a fact in dispute as YGC openly used this information in Dutch litigation, where the Fruit of the Poisonous Tree Doctrine does not exist.

King and Mariya Shvetsova ("Shvetsova") co-founded the business intelligence firm Vantage Intelligence Ltd. ("Vantage"). King, Shvetsova and Eugene Dizenko ("Dizenko"), a managing director at Vantage, all worked together at Diligence and previously conducted business intelligence for the YGC. The CFO of Vantage is Martin Parr ("Parr") [EXHIBIT 24], who was also simultaneously a YGC employee and board member who testified against me at the S.D.N.Y. trial, where he acknowledged being a director of Vantage:

Q: And what company are you a director of that provides business intelligence services?

A: Vantage Intelligence U.K. Ltd. [EXHIBIT 25] P853 lines 5-7

Not only were three of my email addresses targeted and hacked by Azari, but at least one of my colleagues, Dmitri Merinson, who was also being sued by YGC at the direction of Godfrey had his email hacked by Azari. Richard Deitz, a witness who testified on my behalf at the trial, also had his emails targeted by Azari. Stephen P. Lynch, another litigation opponent of Godfrey was also hacked by Azari. Deitz and Lynch are both US citizens. All four of us were targeted during the same time period.

¹⁴ Misamore was subsequently removed from all YGC positions and sued YGC in Texas.

¹⁵ A stichting is a Dutch legal entity with limited liability.

¹⁶ The information harvested from the stolen hard drive was used openly in YGC litigation in the Netherlands, where the fruit of the poisonous tree doctrine does not exist.

¹⁷ EXHIBIT 23 DEED OF DEPOSIT Page 3 lines 24-27. Recounting of a September 2, 2015 conversation between Merinson and Misamore. A tape recording of the conversation was deposited with a notary in Amsterdam, Holland on September 11, 2015.

B. Vantage Intelligence Ltd.

Vantage was co-founded by King, a native of Kansas, who previously worked for seven years at Diligence, a leading international business intelligence firm founded by Nick Day, a former member of MI6.¹⁷ Godfrey was first introduced to King, when she worked on Yukos matters as an employee of Diligence. Ms. King later became Mr. Godfrey's girlfriend and moved to work in-house for Yukos.¹⁸ King shared office space with YGC in London's West End on Kensington High Street where both Theede and Parr, among others, had offices.¹⁹ Theede dined privately with King, including once at the Conservatory Hotel in Amsterdam. Despite this contact and knowledge, Theede during depositions for this case, while under oath testified:

I've never met Gretchen King. I know the name Gretchen King, but have never met Gretchen King. [EXHIBIT 26] P162 lines 9-11.

Theede went on to describe King as:

a service provider who...provides certain information in support of litigation we have ongoing. EXHIBIT [26] P162 lines 23-25.

Theede goes on to say that he presumes that Godfrey hired King and sets her salary. In 2014, YGC paid King's BVI company Notional Holdings over \$1.3 million. In March of 2015, Theede and Misamore were informed via email by Merinson, that Merinson was concerned that King was engaging in or paying for illegal activity and was hesitant to pay her Notional Holdings invoices. Theede instructed Merinson to continue to pay the invoices. YGC also paid for King's office space.

A previous example of King's provision of "certain information" in support of litigation can be found in an email from King to Godfrey²⁰ on December 8, 2011, entitled "*****²¹-male escort", [EXHIBIT 27] which serves as an example of them working together to illegally obtain information. The personal information being provided concerns an individual involved in litigation with the YGC. From the email it appears that King has been able to obtain the individual's cellphone records. The original email [EXHIBIT 27] that King forwarded to Godfrey is from a Matthew Toma a colleague of King's at Diligence and reads as follows:

Hey Gretchen,

Came across this number in *****'s records while he was in the UK...

¹⁷ The UK's Secret Intelligence Service, a British government agency that collects and analyzes foreign intelligence.

¹⁸ As a former close friend of Godfrey's I had firsthand knowledge of this. Additionally, I had dinner with King in New York City's Village where she asked me if she thought she was wasting her time as Godfrey's girlfriend and inquired if I thought Godfrey was serious about their relationship.

¹⁹ As a former YGC employee I was often in London and visited these offices and saw King and Parr in the shared office space.

²⁰ Godfrey then forwarded the email to me.

²¹ I have redacted the name of the person here as their privacy should be respected and have redacted it in the exhibit as well.

It then lists the contact information for a male escort service and concludes with:

***** called 5 times when he was in London.
Thought you might appreciate

Their aim is not only to illegally access business information about litigation opponents but to also gain compromising information on litigation opponents that can be used as leverage. Upon accessing someone's phone records or email accounts, that becomes a possibility.

King describes her time with Yukos on her bio on the Vantage website as:

Gretchen then joined an oil company to establish and lead an in-house intelligence unit; the primary focus of the unit was to provide intelligence and evidence in support of multiple high-value legal disputes...evidence²² gathered by the unit contributed to multiple legal victories." [EXHIBIT 28]

King went on to co-found Vantage with Shvetsova,²³ a former colleague at Diligence who also worked on YGC matters. They appointed Dizenko, a former co-worker at Diligence who worked on YGC matters, as a managing director of Vantage. Vantage shared offices with YGC in London, where YGC accountant and a member of various YGC boards of director Parr worked. Parr held both his YGC roles and his role as CFO of Vantage simultaneously further cementing the commonality of interests between the two companies. Parr testified on behalf of YGC at the S.D.N.Y trial. An organizational chart of Vantage taken from the company's current website lists King²⁴ and Shvetsova as Founders, Dizenko a Managing Director and Parr the CFO; both Parr and Dizenko are part of Executive Management. [EXHIBIT 29]

C. Project Yummy

On January 14, 2025, AUSA Murray sent me via email [EXHIBIT 10] with an FBI agent and Olga Zverovich a Russian speaking AUSA on copy, eight new evidentiary documents with bates numbers, including document AZ_00061410. [EXHIBIT 20] AUSA Murray wrote:

Evidence reflects that you were added to "Project Yummy" as a new target on March 3, 2017 (AZ_00061410).

AZ_00061410 [EXHIBIT 20] hereto, is an email sent, "Fri 3/3/2017 7:49:07 AM (UTC), entitled: **New Target Project Yummy**."²⁵ The body of the email in full reads:

Daniel Caleb Feldman

²² Among the evidence gathered during this time by Ms. King was a copy of the hard drive of Nikita Tolstikov's laptop computer. Mr. Tolstikov was in-house counsel for Rosneft, the Russian government run oil company and a frequent litigation opponent of Yukos. Ms. King obtained the copy of the hard drive, in exchange for \$15,000.

²³ Mariya Shvetsova is at times referred to as Masha Shvetsova.

²⁴ King fled the UK and now resides in the Emirates. She has not returned to the United States for many years. It is my understanding that she fears arrest upon a return to the United States.

²⁵ I do not think that it is a coincidence that Yukos and Yummy begin with the same two letters.

Feldman23@gmail.com
Caleb23@aol.com
 Mobile - +1 646 703 4350

While the sender and receiver names are redacted in AZ_00061410, on March 10, 2025, AUSA Murray confirmed it was an email sent from one of the leaders of BellTroX to one of the BellTroX hackers. [EXHIBIT 11] BellTroX and CyberRoot are the two Indian hack-for-hire groups used by Azari and his criminal associates.

The January 14, 2025, email from AUSA Murray was not the first time the United States government provided me with evidence obtained from the criminal case against Azari. The DOJ shared documents with me via the USAfx file share system. The first batch of documents was uploaded on October 11, 2024. [EXHIBIT 7] This included ninety-four phishing emails [EXHIBIT 29] and eleven invoices from Azari to King's companies Vantage (ten invoices) and Notional Holdings (one invoice). [EXHIBIT 31] Five additional documents were uploaded to the USAfx system on December 17, 2024, at 12:19 pm. [EXHIBIT 8] These included four additional emails and a screen shot of my Address Three email inbox. [EXHIBIT 32] All of these documents were obtained from Azari. On December 17, 2024, at 5:31 pm, AUSA Murray emailed me an Azari cover email, sent on January 18, 2016, that included the attachment of the screenshot of the Address Three inbox. [EXHIBIT 22]. The January 18, 2016, was sent from a known Azari email account using the alias, Poul Kremer²⁶ and includes the following:

Id's used by Daniel Caleb Feldman
caleb23@aol.com (The one we got from the customer)
dan@mondogoal.com
feldman23@gmail.com
feldmand@yukos.ru

See attached total amount of mails between Daniel C. Feldman to the one we have.
 [EXHIBIT 9]

Prior to being added to Project Yummy on March 3, 2017, I was already being targeted by Azari. The first Azari spear phishing email I received, that I am aware of was on January 19, 2016. There are invoices from Azari to King that predate the New Target Project Yummy email. Invoices 104, 107 and 108 [EXHIBITS 31 and 33] are from December 2016. Invoice 104 is sent on 12/1/2016 (Bates # AZ_00185612). [EXHIBIT 34] Invoices 107 and 108 are sent together on 12/29/2016 (Bates # AZ_00096136). [EXHIBIT 34] These invoices were sent from Azari directly to a King email account named DS Project with a full address of dsprojectrussia@gmail.com and the emails with the invoices attached both began with: "Dear Gretchen." Upon being added to Project Yummy, the invoices are sent to King's Vantage email account. The cover emails [EXHIBIT 34] for all of the invoices were sent to me by AUSA Murray on January 14, 2025. [EXHIBIT 10] Invoices 108 and 153 [EXHIBIT 33] were sent to me by AUSA Murray on March 10, 2025. [EXHIBIT 11]

²⁶ For years, including throughout the S.D.N.Y. litigation, the law firm Gibson Dunn & Crutcher ("Gibson") represented YGC in various litigation matters. Throughout this time, Gibson had an of-counsel attorney named Paul Kremer.

D. The Project Yummy Emails

On 3/3/2017 at 12:11:38 PM (UTC), four hours and twenty-two minutes after the *New Target Project Yummy* email, [EXHIBIT 20] a campaign of *phishing emails*²⁷ commenced. [EXHIBIT 30 Bates #AZ_00873654] As included in Exhibits 30 and 32, per the evidence provided to me by the US Attorney's Office, for the month of March 2017, I received at least the following 41 phishing emails from Azari's criminal enterprise:

<u>Date</u>	<u>Number of Emails</u>
3/3/2017	2
3/6/2017	8
3/7/2017	10
3/10/2017	10
3/11/2017	1
3/15/2017	1
3/22/2017	4
3/23/2017	1
3/25/2017	1
3/27/2017	1
3/28/2017	1
3/30/2017	1

On March 21, 2017, Azari's firm Nerosia Ltd. sent an email [EXHIBIT 34 Bates #AZ_00285953] to King's Vantage email address, gk@vantageintel.com with Nerosia Ltd. Commercial Invoice 117 dated March 13, 2017, for €53,000 attached. [EXHIBIT 31] This is King's email address as currently listed on the Vantage Intelligence website. [EXHIBIT 28] Invoice 117 indicates that the customer is *Vantage Intelligence Ltd.* and the Description of Services is *Consulting*. Additionally, there is a hand written note reading:

*The money has been wired to the bank in Malta.

The campaign of phishing emails continued throughout 2017 with at least another twenty-six in April, six in May and eleven in June and at least two more in November per the information provided to me by the US Attorney's Office. [EXHIBITS 30 & 32] Invoices continued to be sent from Azari to King. On April 24, 2017, Azari sent King two emails with Nerosia invoices attached to her Vantage email account. The first at 7:38:41 AM with Invoice 123 [EXHIBIT 34] attached dated April 18, 2017, to customer *Vantage Intelligence Ltd* for *Consulting* with an amount due of €16,000. Just over a minute later at 7:39:49 AM, Invoice 124 [EXHIBIT 34] also dated April 18, 2017, is sent to King with an amount due of €56,000. The customer for Invoice 124 is listed as

²⁷ A phishing email is a fraudulent message that tricks you into giving away personal information. It may appear to come from a legitimate source to increase the likelihood that the email is opened and link is clicked.

Notional Holdings Ltd. [EXHIBIT 31] This is a company also run by King, the predecessor to Vantage Intelligence, and a company closely associated with YGC.

Historically, Notional Holdings Ltd. billed the YGC's Gibraltar company Mojave East Management Pte Limited ("Mojave East") for work done by King.²⁸ Mojave East was a company set up by Godfrey and King that was purposely removed from the YGC's consolidated accounting.²⁹ An invoice dated March 16, 2015, [EXHIBIT 35] issued by Notional Holdings to Mojave East for \$75,000 includes as a description of services:

Fee for M.Shvetsova re work on RC Data collection and Jervis

As mentioned above, Shvetsova is the co-founder of Vantage and is a former member of King's "investigative" team at Diligence. Shvetsova personally invoiced Notional Holdings on March 9, 2015, [EXHIBIT 35] the same \$75,000 with a note that it should be billed to Mojave East. The description of services is listed as "Consulting fee: Investigative services". As detailed below, the YGC was in litigation at that time with Promneftstroy, which was owned by three groups, including Renaissance Capital ("RC") and RC had the contents of their entire server stolen at that time. Bob Foresman was the Deputy CEO of RC and was the target of the RC litigation.³⁰

There was an extended pause before the phishing email campaign began again in September, 2018 with at least 6 more and then at least 4 more in October 2018. The US Attorney's Office provided me with nearly one hundred phishing emails sent by Azari to my email accounts from January 2016 through October 2018. [EXHIBITS 30 & 32] I have listed these emails on an Excel spreadsheet by chronological order. [EXHIBIT 36] I was also provided with a screen shot of my Address Three inbox that was obtained by the government via a warrant from Azari. [EXHIBIT 22] While the US Attorney's Office did not provide me with the phishing emails to my Address Three email address, Reuters News Agency did. [EXHIBIT 21] In addition, the 126 documents I was provided by the US Attorney's Office begin at Bates number AZ_00061410 and go through AZ_02220361, indicating that there are numerous additional documents that I may not have been provided with.

The barrage of emails generally fell into three categories: spoofing³¹ of email addresses of previous work contacts, pornography-related, and social media updates or news stories. The news stories were a mix of random topics and some that the hackers thought I might find interesting. This mix of topic-specific and generic attempts is typically of a hacking campaign. Clicking on any link in the emails triggered a program that would allow the hackers access to my emails, files and computer generally.

²⁸ As a former YGC employee and secretary of the stichting, I have firsthand knowledge of this.

²⁹ As a former YGC employee and secretary of the stichting, I have firsthand knowledge of this. In addition, Mojave paid many invoices of criminal law counsel for King and Godfrey in the UK and the USA.

³⁰ Interestingly, while the other two owners of Promneftstroy, including Deitz whose video testimony was used during my trial, were targeted by Azari's hacking scheme, Foresman was not. I would posit that this was because YGC already had the contents of his email via Notional Holdings, King, Shvetsova and the stolen server contents.

³¹ Spoofing is a cybercrime where someone disguises their identity or communication to appear as a trusted source, often to gain access to sensitive information, steal money, or spread malware.

In the first category, the spear phishing emails appeared to be from David Rourke, John O’Kelly-Lynch and Gary Carr. Rourke, O’Kelly-Lynch and Carr were my contacts at Delphi Management, a little-known Bermuda based fund management company. I had worked with them as they were the fund manager for the UFG Fund in which I had invested YGC money. Two examples of these emails found in documents AZ_00358902 and AZ_00634777. [EXHIBIT 30]

AZ_00358902 is dated June 9, 2017 and the email subject is:

John O’Kelly-Lynch shared “UFG Private Equity Fund” with you

The email purports to share information via a Dropbox link.

AZ_00636477 is dated March 10, 2017, and the email subject and body of the email reads:

Gary Carr has invited you to edit the following document:

Hi, Kindly find the documents and revert back to me please.

Thank you

-Gary Carr

On January 29, 2019, a little over a month prior to the S.D.N.Y. trial, I received a phishing email [EXHIBIT 37] to my Address One account with the subject line:

Yukos Capital SARL Details

Yukos Capital SARL is one of the plaintiffs in the SDNY case. This email included the note that:

David Rourke has sent you an email via Gmail confidential mode”

This email purported to be from little known Delphi employee David Rourke. Only when printing out the email or hovering over his name, can you see that it is not from his work email account. I reached out to Rourke upon receiving the email and he confirmed that he did not send me this. [EXHIBIT 37]

In addition to the above emails, there are surely countless others that were sent to me and were not found by the US Attorney’s Office. Maltin Litigation Support (“MLS”), a UK based firm, provided a list of additional spear phishing emails sent to me. MLS represented a victim, Farhad Azima, of Azari’s hacking schemes and found in their records fifteen additional emails that were sent by Azari to my Address One and Address Two accounts between 1/13/2016 to 3/31/2017. [EXHIBIT 38]³² Five of these were made to appear as though they were from Gary Carr and David Rourke of Delphi Management in Bermuda.

Reuters news agency also sent me a list of eighteen emails from Azari directed accounts to my Address One and Address Three accounts. [EXHIBIT 21] These emails begin on 1/14/2016 and

³² This EXHIBIT is similar to emails provided by Reuters in EXHIBITS 18 and 19.

go through 3/31/2017 and include nine emails to my Address Three (mondogal) account from January to March of 2016.³³

The pornography focused emails typically announced that I had signed up to receive daily pornography and would have to click an unsubscribe button to stop receiving the pornographic emails. There are numerous examples in the attached exhibits, reviewing each in turn would be overly repetitive. I encourage the court to review the exhibits in full but provide the below as examples. I have purposely not selected examples some of the most graphic and offensive emails that were persistently sent to my email address. These include but are definitely not limited to Bates numbered documents AZ_00356266, AZ_00356316, AZ_00636425 and AZ_00634725. [EXHIBIT 30]

Two examples of the not graphic emails that relate to pornography are:

AZ_00634704 from March 6, 2017, reads:

You have been successfully subscribed to Youporn.com
Hello,
You have been successfully subscribed to Youporn.com, your account has been activated.
You can go to Youporn.com to log into your account. Your account information is shown below for reference purposes.
User ID: feldman23@gmail.com

All the best,
Youporn Team.

Note: If you received this email in error and did not sign up for a Youporn account you can simply Unsubscribe this email
[EXHIBIT 30]

Another, AZ_00358985 dated June 12, 2017:

You have been successfully subscribed to Pornhub.com
Thanks for becoming part of the Pornhub service
Your Pornhub account feldman23@gmail.com has been created.
If you received this email in error and did not sign up for a Pornhub account you can simply Unsubscribe this email -- No further emails will be sent to you.
[EXHIBIT 30]

If I ignored the emails, many more would follow. The clear intent behind these emails was to embarrass the recipient into clicking on the unsubscribe link to attempt to stop the mails being sent, which would then compromise their email account.

³³ The eight emails to the feldman23@gmail.com account are duplicative of the eight emails provided to me by MLS in EXHIBIT 38.

Other emails, such as AZ_00357602, [EXHIBIT 30] claimed that a “Rebecca Alessandra Giacchi” had tagged me in a Facebook post stating that she loved me and had a button to click to view the post or unsubscribe from receiving these notifications. I do not know anyone by that name and as a married man, this is an unsettling email to receive and intended to provoke an emotional response, as Facebook posts that tag someone are public and viewable by family and friends.

Numerous other emails included news stories, some that I might find interesting and others that I would not. In both instances, the aim was to induce me to click on the story or the unsubscribe button. Examples of these can be found in Bates numbered documents AZ_00636162, AZ_00359156, AZ_00359168 and AZ_00359183. [EXHIBIT 30]

E. The Invoices

Throughout the illegal phishing campaign, invoices were sent from Nerosia Ltd. (Azari’s Cypriot company) to Vantage. The invoices were included as attachments to emails from Azari to King. Both the emails and the attachments were forwarded to me by AUSA Murray upon my request for information related to the hacking of my email accounts. The invoices and the parties involved provide evidentiary support as to who was paying for the hacking campaign against me throughout the S.D.N.Y. litigation. They total €357,000. The emails and the attached invoices are included in Exhibits 30, 32 and 33.

On January 14, 2025, AUSA Murray sent me an email [EXHIBIT 10] that included the following list:

AZ_00185612 – Cover email for Invoice 104, 12/01/2016
 AZ_00096136 – Cover email for Invoices 107 and 108, 12/29/2016
 AZ_00285953 – Cover email for Invoice 117, 3/21/2017
 AZ_00252940 – Cover email for Invoice 123, 4/24/2017
 AZ_00252995 – Cover email for Invoice 124, 4/24/2017
 AZ_00591172 – Cover email for Invoices 116, 117, 123, 124, 129, 130 and 132.
 Email sent on 10/18/2017 by Azari notes the invoices range from Feb-Sept 2017
 AZ_00591738 – Cover email for Invoices 141, 142, 149 and 153. Email sent on 8/28/2018.

On March 10, 2025, AUSA Murray sent me an email [EXHIBIT 11] with Invoices Number 108 and 153 attached. [EXHIBIT 33] I had not previously been sent these invoices.

The invoices were typically sent to King’s email at Vantage (gk@vantageintel.com) requesting payment from Vantage (or Notional Holdings, an associated entity). Others were sent to Monica Marathefti (“Marathefti”), a Cyprus based accountant, requesting payment from Vantage. The emails were sent from either Nerosia@protonmail or a known Azari alias Poul Kremer. Poul Kremer, was the name associated to the bonbon12@gmail.com email address, which was operated by Azari.

AZ_00185612 is an email sent on December 1, 2016, from a known Azari alias and email address, Poul Kremer <bonbon12@gmail.com> to “DS Project” and begins with the greeting: “Dear

Gretchen.” [EXHIBIT 34] Attached to this email was Invoice 104 to: Vantage Intelligence Ltd. and is for €33,000. [EXHIBIT 31] Both the body of the email and the invoice include wiring instructions to a Nerosia Ltd. bank account at Sata Bank in Malta.³⁴

AZ_00096136 is an email sent on December 29, 2016, from Azari (Poul Kremer) to DS Project and begins with the greeting: Dear Gretchen. [EXHIBIT 34] Attached to the email are invoices 107 and 108 to: Vantage Intelligence Ltd. [EXHIBITS 31 & 33] Invoice 107 is for €33,000. Invoice 108 was provided to me by AUSA Murray via email on March 10, 2025, [EXHIBIT 11] and is for €20,000. Both the body of the email and the invoices include wiring instructions to a Nerosia LTD bank account at the aforementioned Sata Bank.

AZ_00285953 is a cover email for Invoice 117 [EXHIBIT 31] sent on March 21, 2017, from Nerosia@protonmail.com directly to King’s email at Vantage Intelligence; gk@vantageintel.com. [EXHIBIT 34] We know this is King’s email as it is listed as such on the Vantage website. [EXHIBIT 28] Invoice 117 is for €53,000 and includes the handwritten note:

*The money has been wired to the bank in Malta.

The bank listed on this invoice is a Latvian Bank, Baltikums Bank AS, but per the handwritten note it appears that the King / Vantage wired the money to a bank in Malta, where Sata Bank was located. Baltikums Bank changed its name to Blue Orange Bank³⁵ in September 2017. It has a branch in Cyprus where Azari’s company was located.

AZ_00252940 is a cover email [EXHIBIT 32] for Invoice 123 [EXHIBIT 31], sent on April 24, 2017, from Nerosia@protonmail.com directly to Gretchen King’s email at Vantage; gk@vantageintel.com. Invoice 123 is for €16,000.

AZ_00252995 is the cover email [EXHIBIT 34] for Invoice 124 [EXHIBIT 31], sent on April 24, 2017. The amount for this invoice is €56,000. This one like Invoice123, is sent to King’s Vantage email address. However, the invoice is to Notional Holdings not Vantage. While the link between King, Vantage and Notional Holdings is well known, this further evidences the link.

Invoices 129, 130 and 132 [EXHIBIT 31] sent from Azari to Marathefti, on October 18, 2017. [EXHIBIT 34] Invoices 141, 142, 149 and 153, [EXHIBITS 31 & 33] were sent from Azari to Marathefti on August 28, 2018. [EXHIBIT 34] Each of these invoices include wire instructions to the Nerosia account at Sata Bank and the customer is listed as Vantage Intelligence Ltd. They were for a total of €146,000 and spanned from July 10, 2017, to June 26, 2018. Invoice 149 includes Vantage’s office address in London, 25 Old Burlington Street, London W1S 3AN. [EXHIBIT 31]

³⁴ Sata Bank was shuttered in 2018 due to widespread breaches of money laundering laws and has since lost its banking license as billions of euros were moved through the bank in suspicious transactions.

³⁵ In 2018, Latvia’s banking watchdog fined BlueOrange Bank 1.2 million euros for violating anti-money laundering and terrorism financing rules. The breaches related to the bank’s operations in 2016 and 2017 when operating as Baltikums Bank, largely served non-resident clients mainly from former Soviet Union countries.

F. July 13, 2017 Amended Complaint

On July 13, 2017, YGC filed an amended complaint in the present S.D.N.Y. case, adding to their list of claims what has been referred to as the Julius Baer bank claim and is listed on the verdict form as Claim 1, [EXHIBIT 1] alleging a breach of fiduciary duty. This is one of the two claims where the jury ruled that I had breached my fiduciary duty. The claim is focused on a payment from Julius Baer to Merinson. Both Merinson and I were victims of Azari's hacking and provided victim impact statements at Azari's sentencing hearing in the S.D.N.Y. before District Judge Hon. John G. Koetl. The email adding me to Project Yummy [EXHIBIT 20] was sent on March 3, 2017. Hours later I began receiving spear phishing emails from the hackers. Per the information provided to me by the US Attorney's Office, I received at least eighty-eight phishing emails from Azari between March 3, 2017 through June 14, 2017. [EXHIBITS 30, 32 & 36] The complaint was amended on July 13, 2017. On June 14, 2017, the phishing emails appear to have abruptly stopped until I received two more on November 28, 2017, and then a ten month pause until September and October of 2018, when I received another thirteen phishing emails from Azari in the months leading up to the S.D.N.Y. trial. [EXHIBIT 30, 32 & 36]

There is indisputable evidence that Azari was hacking into both my and Merinson's email accounts just prior to YGC amending the complaint; then the hacking immediately paused for an extended period.

G. Links Between the Yukos Group Companies and Aviram Azari

From 2015 onwards, I was in litigation with Yukos and YGC in SDNY. The case went to trial in March 2019, and continued with appeals following judgment.

On April 3, 2017, I was added to the list of 'targets' for 'Project Yummy', a matter on which Azari worked. The campaign explicitly targeted the Address One and Address Two accounts. [EXHIBIT 20] Based on the screen capture of the Address Three account [EXHIBIT 22] that was provided by the US Attorney's Office, it is clear that the efforts to hack into my private information began in 2016, prior to Project Yummy, and that Project Yummy expanded the illegal campaign or Azari added a new Indian hacking company. The screen capture demonstrates that the efforts to illegally access my emails were successful [EXHIBIT 22] as does the continued engagement of Azari by Vantage and King evidenced by the invoices that total €357,000. [EXHIBITS 31 & 33] One does not engage and continue to pay a service provider for years if results are not being achieved.

As detailed above and exhibited hereto, I have been provided with emails and invoices from the DOJ relating to the phishing campaign that took place against me. The invoices I have been provided with run from January 12, 2016, through August 28, 2018, and were billed to either Vantage or its associated company, Notional Holdings and were all sent to King. Vantage is run by former YGC employees King and Parr, and payments from YGC to Vantage and Notional Holdings were made through an entity purposely placed outside the YGC company structure, Mojave East. Martin Parr, a longtime YGC accountant and board member of YGC companies testified for the plaintiffs at the S.D.N.Y. trial before the Hon J. Kaplan and was at the time and is still a director and the CFO of Vantage. [EXHIBITS 24, 25 & 29]

The spear phishing emails within Azari's campaign utilized spoof senders by which the emails claimed to come from members of the team at Delphi Management. [EXHIBIT 30³⁶, 37 & 38] My involvement with Delphi Management related to YGC funds that I had invested, and was known to a very small group of individuals and companies, including YGC. The use of spoof senders relating to Delphi Management is a clear indicator that material was being provided by Azari's client to inform the hackers' campaign.

Dmitri Merinson, Richard Deitz and Stephen P. Lynch were all potential witnesses in my case. Deitz was deposed leading up to the trial. Deitz's deposition video was used in lieu of live testimony at the trial. All three had their emails targeted and / or hacked by Azari during the S.D.N.Y. litigation. [EXHIBIT 39] All three were also in direct litigation with YGC contemporaneous to the S.D.N.Y. litigation. On November 17, 2023, in the S.D.N.Y. before the Hon. J. John Koetl, Merinson provided a written victim impact statement that was added to the record of Azari's sentencing hearing.

Bruce Misamore, the former CFO of Yukos and former board member of the Dutch stichtings and many YGC companies, informed Dmitri Merinson that Godfrey, former General Counsel of Yukos and board member of the Dutch stichtings, steals information from laptops to deploy in Yukos related litigation. [EXHIBIT 23]

An invoice dated March 16, 2015, was issued by Notional Holdings to Mojave East for \$75,000, [EXHIBIT 35] including a description of services:

Fee for M.Shvetsova re work on RC Data collection and Jervis

Shvetsova is the co-founder of Vantage [EXHIBIT 29] and is a former Diligence colleague of King. The Notional Holdings invoice was issued when YGC was in litigation with Promneftstroy, which was partially owned by Renaissance Capital. It is a clear inference to draw that 'RC' in the Notational Holdings invoice refers to Renaissance Capital. Included in EXHIBIT 35, is Shvetsova's personal invoice for services dated March 9, 2015, to Notional Holdings, with instructions that Mojave East should receive a bill for \$75,000.

Reuters Investigates news articles written by Bing and Satter reveal that Azari's typical clients are Jewish Russian oligarchs with ties to Israel. This matches the profile of YGC ultimate beneficiaries, Russians Leonid Nevzlin, Mikhail Brudno and Vladimir Dubov who all now live in Israel.

Throughout the litigation process the email accounts that I used to communicate with my attorneys were targeted by Azari. [EXHIBIT 3] I was involved in no other litigation at the time. Based on the evidence provided by the DOJ relating to payments to Azari made by business intelligence firms closely associated with YGC, and the deployment of spoof senders clearly related to my dispute with YGC, it is also clear to infer that Azari's phishing campaign was undertaken for the sole benefit of YGC.

³⁶ AZ_00634777, AZ_00634821, AZ_00636477, AZ_00636508, AZ_0000358902

As such, YGC accessed material from my email accounts that was covered by Attorney Client Privilege, likely informing their litigation strategy and thus irrevocably tainting the entire litigation process. The material which would have been seen by the hackers, and by YGC, included drafts of motions, strategy and similar. [EXHIBIT 3] This is clearly prejudicial and created an unfair advantage for the plaintiffs in this case.

As a result, of the tainting of the litigation process and the affront to justice that this presents, the judgments of March 19, 2019, reflected on the Verdict Form as Claims 1 and 5 [EXHIBIT 1] must be set aside with prejudice.

The picture is clear. I was in a business dispute with only YGC. YGC hired Azari to hack into my emails during the litigation process. Azari was hired to hack into three of my email addresses, three contemplated witnesses of mine and others in litigation with YGC in other cases outside of the United States. Azari's typical clients exactly match those with whom I was in litigation. The timing of the crimes mirrors the S.D.N.Y. litigation timeline. Email was my primary means of communication with my attorneys. Drafts of motions, strategy and much more were all shared via email as well as communications with expert witnesses and litigation strategy. It belies sense that it did not create an unfair advantage for the plaintiffs that would taint the result of the litigation.

Equanimity is the hallmark of the US judicial system. Equanimity and justice demand that the judgment be set aside with prejudice.

H. Fraud Unravels All / Farhad Azima

Farhad Azima ("Azima") is another victim of Azari's hacking during a business litigation. Azima's litigation history provides an example of how common law jurisdictions view such behavior. A review of his case presents an amazingly factually similar case to my case. In 2016, a year after YGC filed the S.D.N.Y. case, Azima, a Missouri based American aviation executive, was sued in the High Court of England and Wales ("High Court") by his former business partner Ras Al Khaimah Investment Authority ("RAKIA"), a United Emirates investment fund. In 2020 the High Court found in favor of RAKIA and a judgment was entered against Azima for more than \$4 million.

Subsequently, in March 2024, the High Court set aside the original judgment of more than \$4 million against Azima, and ordered RAKIA who used Azari's hacking services, to pay Azima over \$10 million in litigation costs, interest and damages. [EXHIBIT 40] Azima has since filed cases in the United States in the S.D.N.Y, North Carolina and Florida to hold those responsible accountable for hacking campaign that targeted him. Those cases are ongoing. The way this turn of events occurred is nearly identical to the path my case has followed.

Azima uncovered who was responsible for his hacking in a similar manner to myself. In 2020, Satter and Bing, two Reuters journalists investigating a group of Indian hackers who specialized in stealing emails to sway court cases in favor of their clients, reached out to Azima to ask if he knew why his email address was targeted by the Indian hackers. From there, Azima was able to prove to the High Court that RAKIA had been responsible for his hacking, resulting in the judgment against him being overturned. Mr. Justice Michael Green ruled that RAKIA's conduct

was egregious and found that the, **“fraud unravels all” principle outweighs the finality principle**” in the context of setting aside a judgment. [EXHIBIT 41, P25, ¶131]

On July 7, 2022, Bing reached out to me [EXHIBIT 13] for the same purpose Bing and Satter reached out to Azima, to ask if I knew why I had been the target of a hacking by Azari. After I spoke with Bing and Satter, I reached out to the U.S. Attorney’s Office. I met with them in person numerous times, provided a victim impact statement at Azari’s sentencing and have since been in regular contact with them. With the US Attorney’s Office and the FBI’s assistance, I have obtained numerous documents that are included here as exhibits that tie the hacking of my emails to YGC.

In the High Court’s 2024 decision overturning the original finding against Azima, High Court Justice Michael Green stated that it was an, “egregious case” and that due to the hacking, RAKIA had, “obtained judgments by fraud.” [EXHIBIT 42, Page 2, lines 19-21] The initial decision was thrown out as Azima’s litigation opponent had covered up its use of hackers to steal the Azima’s emails in order to win the case.

As with RAKIA, it is only just that YGC does not profit or benefit in any form from their decision to deploy underhanded and illegal methods to gain an advantage in litigation.

I. Procedural Background

A jury trial in the S.D.N.Y took place before the Hon. L. Kaplan, with a decision rendered March 19, 2019. Eight of the ten claims were rejected by the jury. [EXHIBIT 1] For two claims I was found to have breached a fiduciary duty but caused no harm. No finding of fraud was made by the jury. The jury rejected the claim that I had acted with venal intent. The Hon. Judge Kaplan imposed nominal fines of \$1 per plaintiff per breach.

Both plaintiffs and the defendant filed appeals. The appeal was argued on February 20, 2020, with the decision handed down on October 13, 2020. The trial court findings were upheld, but the breaches against two of the plaintiffs, the stichtings, were dismissed.

III. LEGAL ANALYSIS

Federal Rule of Civil Procedure 60(b), first adopted in 1937, empowers a court to relieve a party from a previous judgment. A motion filed more than ten days after the entry of judgment, is properly filed as a motion seeking relief from judgment under Rule 60(b). *McMillion v. District of Columbia*, 233 F.R.D. 179, 179 n.1 (D.D.C. 2005). The court analyzing a motion under Rule 60(b) and in its discretion, may relieve a party from an otherwise final judgment. FRCP 60(b); *Lepkowski v. U.S. Department of Treasury*, 804 F.2d 1310, 1311-12 (D.C. Cir. 1986). The rule provides for setting aside a judgment for any one of five specified reasons with a sixth being for “any other reason” that justifies relief from the judgment. Upon satisfaction one of the six bases, Rule 60(b) empowers a court to exercise its considerable discretion to counteract injustice.

A. Legal Standard for Relief Under Federal Rule of Civil Procedure 60(b): Reasonable Time

To proceed under Rule 60(b)(1-3), the motion must be filed within one year from the judgment. As that time has passed, I must rely on one of the remaining three reasons and do so within a *reasonable time*. (FRCP 60(c)(1) (A motion under Rule 60(b) must be made within a reasonable time—and for reasons (1), (2), and (3) no more than a year after the entry of the judgment or order or the date of the proceeding.) As detailed below, I seek to have the judgments set aside pursuant to FRCP 60(b)(6), which includes, *any other reason that justifies relief*. I recognize that the use of this sixth option is to be used sparingly and courts only apply it in, “extraordinary circumstances.” *Pioneer Investment Services Co. v. Brunswick Associates Ltd. Partnership*, 507 U.S. 380, 393 (1993) (To justify relief under subsection (6), a party must show “extraordinary circumstances” suggesting that the party is faultless in the delay. See *ibid.*; *Ackermann v. United States*, 340 U.S. 193, 197-200 (1950); *Klapprott v. United States*, 335 U.S. 601, 613-614 (1949). If a party is partly to blame for the delay, relief must be sought within one year under subsection (1) and the party's neglect must be excusable. In *Klapprott*, for example, the petitioner had been effectively prevented from taking a timely appeal of a judgment by incarceration, ill health, and other factors beyond his reasonable control. Four years after a default judgment had been entered against him, he sought to reopen the matter under Rule 60(b) and was permitted to do so. As explained by Justice Black:

“It is contended that the one-year limitation [of subsection (1)] bars petitioner on the premise that the petition to set aside the judgment showed, at most, nothing but ‘excusable neglect.’ And of course, the one-year limitation would control if no more than ‘neglect’ was disclosed by the petition. In that event the petitioner could not avail himself of the broad ‘any other reason’ clause of 60(b). But petitioner’s allegations set up an extraordinary situation which cannot fairly or logically be classified as mere ‘neglect’ on his part.”)

The delay here is not due to neglect and any limitations issue that I am now facing was outside of my control. By nature, a hacking campaign is a covert operation.

What constitutes reasonable time, “must of necessity depend upon the facts in each individual case.” *M.A.S. v. Mississippi D.H.S.* 842 So. 2d 527, 530 (2003). Relevant factors include whether the movant’s delay prejudiced the nonmoving party and whether there is a good reason for the movant’s delay. *Id.* In the present case, there is indeed good cause for delay. The plaintiffs employed illegal tactics that were by design extremely difficult to uncover. In fact, only a fortuitous tip-off from investigative journalists and subsequent engagement with the DOJ revealed that I was the victim of hacking. Upon being notified of the hacking, I began working with the US Attorney’s Office and the FBI to see what else could be uncovered. Since receiving the aforementioned email from Reuters in July 2022, [EXHIBIT 13] I have expeditiously put together the information utilized in this motion. I received new documentary evidence from the DOJ as recently as March 10, 2025. [EXHIBIT 11] To argue that I should have become aware of the actions that have led to this motion earlier, is counterfactual. Not knowing did not involve neglect on my part. There is no prejudice for the nonmoving party here as they were awarded \$1 per breach and my actions were adjudicated to have caused them no harm.

By its very nature, the contracting of Indian hack-for-hire firms was a concealed act. Such companies do not advertise their services, and certainly do not publish a list of their clients or the matters in which they are involved. It was only the involvement of investigative journalists and cooperation with Federal agencies that enabled me to uncover the crimes committed against me. The lengths to which the retention of Azari was hidden also highlights the clandestine nature of his work. Payments to Azari were routed through a company not formally part of the YGC (Mojave East), through Vantage (or Notational Holdings), through to Azari. In at least two instances, the invoice was sent from Azari using a known to law enforcement alias (Poul Kremer). [EXHIBIT 34]³⁷ The complexity of this structure, as well as the necessary secrecy in undertaking illegal actions, would have made any earlier efforts on my part to allege that plaintiffs had commissioned the successful hacking of my data appear fanciful at best. As it is, I have waited until I received as much evidence as I feel possible from the DOJ to ensure I can present a coherent description of the actions of YGC before seeking to set aside the judgment against me.

Although subsection (6) of FRCP 60(b) does not include an official time limit, courts are quick to dismiss motions where the losing party does not file its motion promptly after learning about the circumstances upon which the motion will be based. Thus, I am confronted with the difficult decision whether to wait for the criminal investigative process to play out with Azari associate Amit Fortlit,³⁸ hoping he decides to be a cooperating witness and run the risk of the court ruling against my motion for not meeting the reasonableness time requirement. I have decided that the risk of being time barred is not worth it. Finally, on this point, I did not want to reveal my connection with the FBI and the US Attorney's Office until after I provided my victim impact statement at Azari's sentencing hearing on November 17, 2023. This is particularly salient as in 2013 a threat against my life was made by a close associate of Godfrey and fellow member of the YGC Stichting board and involved a Russian Oligarch living in Israel. [EXHIBIT 23, P2 (page 3 of the exhibit) lines 27-30]. Furthermore, Erik Prince, the notorious Blackwater founder, was appointed a board member of Vantage in January, 2024 [EXHIBIT 29], which has me concerned that he could use his considerable influence with the current administration to dissuade the DOJ from cooperating with any investigation in to Vantage's actions.

**B. Legal Standard for Relief Under Federal Rule of Civil Procedure 60(b):
Considerable Discretion and Extraordinary Circumstances**

Rule 60(b)(6) gives the court ample power to vacate a judgment whenever such action is appropriate to accomplish justice. *Pierre v. Bemuth, Lembeke Co.*, 20 F.R.D. 116 (S.D.N.Y.1956). It grants the court significant discretion. One often cited appellate decision refers to it as, "a grand reservoir of equitable power to do justice in a particular case." *Pierce v. Cook & Co. Inc.*, 518 F.2d 720, 722 (10th Cir. 1995), cert. denied, 423 U.S. 1079 (1976), quoting *Radack v. Norwegian America Line Agency, Inc.*, 318 F.2d 538, 542(2d Cir. 1963); *MAS v. Miss. DHS*, 842 So.2d 527, 530 (2003). Given the rule's flexibility, it is tempered by a stringent standard, and accordingly courts will grant relief only in the most extraordinary circumstances and only when such action is necessary to accomplish justice. *Klapprott v. United States*, 335 U.S. 601 (1949); *Ackermann v. United States*, 340 U.S. 193 (1950); *see also Gonzalez v. Crosby*, 545 U.S. 524, 535 (2005); *Liljeberg v. Health Services Acquisition Corp.*, 486 U.S. 847, 863 (1988) (Rule 60(b)(6) "should

³⁷ AZ_00185612 and AZ_00096136

³⁸ Fortlit is currently fighting an extradition request from the US Attorney's Office from the United Kingdom.

only be applied in ‘extraordinary circumstances’”); *Lyons v. Jefferson Bank & Trust*, 994 F.2d 716, 729 (10th Cir. 1993). The 10th Circuit has found extraordinary circumstances to be present when, for example, after entry of judgment, “events not contemplated by the moving party render enforcement of the judgment inequitable.” *Id.*, citing *Zimmerman v. Quinn*, 744 F.2d 81, 82-83 (10th Cir. 1984) and *In re Gledhill*, 76 F.3d 1070, 1081 (10th Cir. 1996).

There are times when *exceptional circumstances* arise, and once such circumstances are shown, 60(b)(6) relief should be granted liberally. When confronted with seemingly inequitable conduct that could only be discovered post-judgment, courts should turn to this, “grand reservoir of equitable power to do justice” in a particular case. I posit that the conduct in the present case is the archetype for the application of Rule 60(b)(6) and that the demands for equanimity in the courts call for the judgments to be set aside with prejudice. My emails with my attorneys were hacked during litigation on behalf of the counterparty by an Israeli covert surveillance expert; this would seem to meet the level of *exceptional circumstances*. I cannot find an analogous fact pattern in a precedent case, which further supports the exceptional nature of these circumstances. However, the case of Farhad Azima in the High Court of England and Wales provides guidance on how seriously the hacking of a party within litigation is treated on other common law jurisdictions. I was deeply moved by Mr. Justice Michael Green’s observation in his High Court decision, that the **“fraud unravels all” principle outweighs the finality principle** in the context of setting aside a judgment. [EXHIBIT 41, P25, ¶131]

C. Balancing of Harms

In balancing the potential harm that a set aside would create, the scales weigh heavily toward setting aside the judgments. YGC was awarded \$2. The loss of \$2 would have no impact on a company with billions of dollars at its disposal. Not setting aside the verdict would implicitly condone the illegal behavior that pervaded the case from the plaintiff’s side, which could impact the public’s perception of justice in the court system.

Setting aside the verdict would also support equanimity and would remove a massive mark against me that can now be seen was the result of a corrupted process. It has been debilitating to my career and my ability to support my family for me to have these two breaches on my record. Removing them, would be life altering. For example, based on the judgment at hand Godfrey, himself a member of the NY Bar, filed a complaint against me with New York’s Attorney Grievance Committee (“AGC”). Based on this fraudulently obtained verdict the New York Supreme Court collaterally estopped me from arguing the facts of the case during the AGC hearing. As a result, in June of 2024, my law license was suspended for one year.

The New York Supreme Court collateral estoppel ruling was made prior to me being made aware of the hacking crimes. Subsequently, the AGC was made aware of the hacking prior to the grievance hearing, but chose to proceed anyway and made it clear that they would only stop if the judgment was set aside.

In September 2024, the New York Supreme Court in Suffolk County ordered me to pay nearly \$40,000 of YGC’s court costs for a case in the Netherlands where I sought to enforce my Directors and Officers Insurance to cover the litigation costs in the present case, where I successfully

defended eight of the ten claims. Due in part to the finding of the two breaches of fiduciary duty here in the S.D.N.Y., the Dutch courts refused to allow coverage under the D&O policy.

Public perception of the justice system is also a relevant consideration here. When considering a Rule 60(b) motion, courts are often concerned with the impact the ruling will have on the public perception of the judicial system. See, e.g., *United States v. 7108 W. Grand Ave.*, 15 F.3d 632, 634 (7th Cir. 1994); *Carter v. Albert Einstein Medical Center*, 804 F.2d 805, 808 (3rd Cir. 1985). In my view, not setting aside these judgments with prejudice would send a message to the public that the court condones YGC's illegal behavior. To allow a judgment to stand where one side has engaged in such abhorrent fraudulent behavior sends the wrong message and creates uncertainty as to the fairness and robustness of the US legal system. It would be analogous to a casino not returning losses to poker table participants where one participant was able to see other players' cards. The cheating on its face would have to be condemned by the casino.

If the court decides to support my motion to set aside the judgment, I pray that the court does so with prejudice, so as to not reward criminal behavior. YGC should not be afforded another opportunity to advance their case. As a threshold issue, I cannot afford another trial. I am writing this motion pro se, as I cannot afford counsel at this time. Allowing another trial would also not cure the harm done. Plaintiffs have already accessed communication that they were not supposed to be privy to, much of it covered by attorney-client privilege. I successfully defended eight of the ten claims. Giving them another chance at any or all of those would not be in the interest of justice and instead would reward their illegal acts. Allowing the two claims at issue to be tried again would not punish the opposing party for their actions as Plaintiffs cannot unknow what they already learned from reading all of my emails. They have access to nearly unlimited money. The plaintiffs would also be thrilled to drive me further into debt in my efforts to defend myself. The outcome would not be relevant to them, they would have already won.

D. Not Relitigating or Seeking a Review of a Trial Court Ruling

I am not seeking to relitigate the case or overturn a judicial ruling, which makes FRCP 60(b) the proper vehicle for my motion. FRCP 60(b) does not give a party the opportunity to re-litigate its case after the court has rendered a decision. *Servants of the Parcels v. Doe*, 204 F.3d 1005, 1012 (10th Cir. 2000); *Voelkel v. General Motors Corp.*, 846 F.Supp. 1482, 1483 (D.Kan 1994) (A Motion to reconsider is not a second opportunity for the losing party to make its strongest case or to dress up arguments that previously failed.), *aff'd*, 43 F.3d 1484 (10 Cir. 1994). Nor is it the purpose of F.R.C.P. 60(b) to allow the court to "revisit the issues already addressed" or consider "new arguments or supporting facts which were otherwise available for presentation" in the underlying proceedings. *Van Skiver v. United States*, 952 F.2d 1241, 1243 (10th Cir. 1991). Thus, unlike FRCP 50 and 59 motions, FRCP. 60(b) motions may be heard and determined by a judge other than the judge who presided over the trial. An FRCP. 60(b)(6) motion demands no review or previous knowledge of the facts. The trial judge has knowledge of the case, which theoretically could influence judgment of this discrete motion, which requires only a review of the exceptional circumstances.

As a properly filed FRCP. 60(b) motion does not seek judicial review of the trial judge's decision, is not intended to address a trial court's errors of law, and it is not being used as a substitute for actual appeal, this motion can be properly addressed by a judge other than the trial judge. While

not controlling here, the State Court of Appeals in North Carolina ruled, “A 60(b) order does not overrule a prior order but, consistent with statutory authority, relieves parties from the effect of an order.” *Charns v. Brown*, 129 N.C. App. 635, 639 (1988). Thus, the general rule that one trial judge may not overrule another does not apply to proper Rule 60(b) motions. *Hoglen v. James*, 38 N.C. App. 728, 731 (1978); *Charleston Cap. Corp. v. Love Valley Enters., Inc.*, 10 N.C. App. 519 (1971). Recitation or knowledge of the facts is not needed or relevant to this motion.

The importance of the finality in litigation has already been seen, in the above cited case of Farhad Azima in England and Wales, to be no barrier to overturning of previous judgments were there has been a manifest perversion of the litigation process. I would argue, based on the information set out above, that this case should be treated in a similar way.

E. Attorney-Client Privilege and Work Product

United States courts recognize the importance, value and sanctity of the attorney-client relationship. “It is essential to the ends of justice that clients should be safe in confiding to their counsel the most secret facts, and to receive advice and advocacy in the light thereof without peril of publicity. Disclosures made to this end should be as secret and inviolable as if the facts had remained in the knowledge of the client alone.” *Continental Casualty Co. v. Pogorzelski*, 275 Wis. 351, 353 (1957) (quoting *Bruley v. Garvin*, 105 Wis. 625, 81 N.W. 1038 (1900)). See also *Jacobi v. Podevels*, 23 Wis. 2d 152, 157, 127 N.W.2d 73 (1964). The concept of “privilege” is critically important in the United States legal system and litigation. Privileged documents and communications are protected and may not be discoverable by an adverse party. Generally, confidential communications between attorneys and clients concerning legal advice are privileged under the doctrine of attorney-client privilege. [Federal Rule of Evidence 502] A party’s documents and notes-including those of the parties’ representatives and attorneys-made primarily in anticipation of litigation are privileged under the work product doctrine. FRCP 26(b)(3). Unlike attorney-client privilege, which focuses on the confidential communications provided by a client to an attorney, the work product doctrine focuses on tangible documents containing the thoughts and mental impressions of an attorney. To invoke work product privilege, documents must not have been created in the ordinary course of business-they must have been prepared primarily in anticipation of litigation. Both work product and privileged documents were included in my emails with my attorneys. The email addresses hacked by Azari contained numerous drafts of filings and thoughts in anticipation of trial. [Exhibit 3]

The proverbial Five C’s test has been met. Attorney-client privilege protects information from discovery of the “5 C’s”: (1) the information was delivered Confidentially; (2) the information was delivered as a Communication; (3) the information was delivered by or to Counsel (an attorney); (4) the information was delivered by or to a Client; and (5) the information was delivered for the purpose of giving or receiving Counsel (legal assistance). Restatement (Third) of the Law Governing Lawyers §68 (Am. Law. Inst. 2000). All five of the C’s occurred with my email correspondence with my attorneys.

IV. CONCLUSION

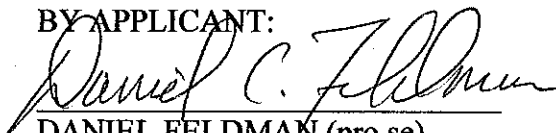
It would be profoundly unjust to let judgments stand where, during the course of the litigation a party illegally hacked into the opposing party's emails, gaining access to their communications including those with their lawyer. The attorney-client relationship and privilege are bedrocks of the US justice system. The fraudulent contumacious misconduct by YGC was part of a litigation strategy that continued for years and was particularly egregious. Lesser sanctions cannot rectify the harm done as they wrongfully and purposefully gained access to otherwise unavailable information that created extreme prejudice. Allowing these abuses to stand is an affront to all aspects of equanimity that we strive to uphold and would create public mistrust in the judicial system. Cheaters and fraudsters should not win and should not be rewarded. They will be if these two judgments are not set aside or are set aside without prejudice. The public also must be assured that crime does not pay. To achieve justice, the two judgments must be set aside with prejudice.

I provided a victim impact statement at Azari's sentencing hearing. The hackers had my Address Three account inbox. The hacking campaign against me continued over a period of years and Vantage continued to pay hundreds of thousands of Euros, totaling €357,000, to the Azari for the entirety of the litigation period. It would belie common sense to think that payments and hacking would continue if positive results and deliverables were not being achieved.

Should this court agree to overturn the verdicts, I would posit that such a decision would not by itself be sufficient and that it would not serve as a deterrent for YGC in future litigations nor others contemplating such illegal activities. For the purposes of deterrence, so that this is not done again, I would pray that the court orders that YGC and the other plaintiffs are liable for all of my legal expenses, including attorneys' fees and that the court impose meaningful punitive damages. The bad actors in this case are each worth over \$100 million and YGC has access to billions of dollars. Although outside of this court's jurisdiction, I humbly suggest that the England and Welsh High Court's decision in the Farhad Azima case can be used for guidance in this instance.

Dated April 10, 2025
New York, NY

RESPECTFULLY SUBMITTED PRO SE
BY APPLICANT:


DANIEL FELDMAN (pro se)

2600 Netherland Avenue, Apt. 820
Bronx, NY 10463
(646)703-4350
daniel@buildingblock.io

Sworn to before me this 10 day
of April, 2025


Notary Public

ANNA COHEN
Notary Public, State of New York
Reg. No. 01CO0032046
Qualified in New York County
Commission Expires 12/17/2028

EXHIBIT

1

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

----- x
YUKOS CAPITAL S.A.R.L., et al.,

Plaintiffs,

15-cv-4964 (LAK)

-against-

DANIEL CALEB FELDMAN,

Defendant.
----- x

*Nominal
Damages*

VERDICT FORM

Breach of Fiduciary Duty ("Julius Baer Scheme")

1. Has each plaintiff listed below proved, by a preponderance of the evidence, that Mr. Feldman breached his fiduciary duty to it by approving Julius Baer's payment of a finders fee to Mr. Merinson?

(i)	Yukos Capital	Yes <u>X</u>	No _____
(ii)	YukosHydrocarbons	Yes <u>X</u>	No _____
(iii)	Foundation I	Yes <u>X</u>	No _____
(iv)	Foundation II	Yes <u>X</u>	No _____

[Proceed to Question 2.]

Breach of Fiduciary Duty ("Promneftstroy Scheme")

2. Has each plaintiff listed below proved, by a preponderance of the evidence, that Mr. Feldman breached his fiduciary duty to it:

- (a) When he was negotiating a potential litigation settlement with Promneftstroy in 2008-2009?

(i)	Yukos Hydrocarbons	Yes _____	No <u>X</u>
(ii)	Foundation I	Yes _____	No <u>X</u>

2

- (iii) Foundation II Yes _____ No X
- (b) By sharing confidential information with Promneftstroy in 2014 and 2015?
- (i) Yukos Hydrocarbons Yes _____ No X
- (ii) Foundation I Yes _____ No X
- (iii) Foundation II Yes _____ No X

[Proceed to Question 3.]

Breach of Fiduciary Duty ("Bonus Scheme")

3. Has each plaintiff listed below proved, by a preponderance of the evidence, that Mr. Feldman breached his fiduciary duty to it by sharing confidential information regarding bonuses with his fellow directors and seeking to establish the secret bonus pool?

- (i) Yukos Hydrocarbons Yes _____ No X
- (ii) Foundation I Yes _____ No X
- (iii) Foundation II Yes _____ No X

[Proceed to Question 4.]

Breach of Fiduciary Duty ("Intelligent Energy Scheme")

4. Has plaintiff Foundation I proved, by a preponderance of the evidence, that Mr. Feldman breached his fiduciary duty to it by attempting to buy the Intelligent Energy shares held by Yukos International U.K. B.V. for his own benefit and against its interest?

Yes _____ No X

[Proceed to Question 5.]

Breach of Fiduciary Duty ("Trust Scheme")

5. Has plaintiff 2015 Security Trust proved, by a preponderance of the evidence, that Mr.

Feldman breached his fiduciary duty to it by withdrawing \$500,000 out of the trust's bank account and investing it in the UFG fund in his own name?

Yes X No

[Proceed to Question 6.]

Breach of Fiduciary Duty ("Georgiades Payments Scheme")

6. Has plaintiff Yukos Hydrocarbons proved, by a preponderance of the evidence, that Mr. Feldman breached his fiduciary duty in connection with:

(a) The Georgiades campaign contribution?

Yes No X

(b) The \$1 million indemnification transfer to Mr. Georgiades?

Yes No X

[Proceed to Question 7.]

Breach of Fiduciary Duty ("Compensation Overpayment Scheme")

7. Has plaintiff Yukos Hydrocarbons proved, by a preponderance of the evidence, that there was an over-payment and that Mr. Feldman breached his fiduciary duty to it by failing to notify it of and return any such over-payment?

Yes No X

[Proceed to Question 8.]

Breach of Fiduciary Duty ("Expense Reimbursement Scheme")

8. Has plaintiff Yukos Hydrocarbons proved, by a preponderance of the evidence, that Mr. Feldman breached his fiduciary duty to it in seeking reimbursement for airline tickets without disclosing that he traveled on less expensive tickets?

Yes No X

[If you answered "Yes" to any of Questions 3.(i), 6.(a), 6.(b), 7 or 8, then you must proceed to Question 9, which addresses the issue of damages. If you answered "No" to each of those Questions, then you should skip Question 9 and proceed to Question 10.]

Damages for Breach of Fiduciary Duty – Compensatory

[Answer Question 9 only if you answered "Yes" to Questions 3.(i), 6.(a), 6.(b), 7 or 8.]

9. Enter the amount of actual damages, if any, that Yukos Hydrocarbons has proved, by a preponderance of the evidence, as a result of the following alleged breaches of fiduciary duty to it:

<u>Scheme</u>	<u>Amount of Damages (if any)</u>
---------------	-----------------------------------

[Answer Question 9.(a) only if you answered "Yes" to Question 3.(i).]

- (a) The "Bonus Scheme"

X

[Answer Question 9.(b) only if you answered "Yes" to Questions 6.(a) or 6.(b).]

- (b) The "Georgiades Payments Scheme"

X

[Answer Question 9.(c) only if you answered "Yes" to Question 7.]

- (c) The "Compensation Overpayment Scheme"

X

[Answer Question 9.(d) only if you answered "Yes" to Question 8.]

- (d) The "Expense Reimbursement Scheme"

X

[Proceed to Question 10.]

Faithless Servant and Other Damages

[Answer Question 10 only if you answered "Yes" to any one of Questions 1 through 8 (including their any sub-parts). If you answered "No" to each of Questions 1 through 8 (including their sub-parts), then you should skip Question 10 and sign your names to the verdict form]

10. (a) Has each of the plaintiffs listed below proved, by a preponderance of the evidence, that Mr. Feldman acted disloyally in substantial respects in his performance of his

services to that particular plaintiff by engaging in any of the schemes for which you earlier found a breach of fiduciary duty?

[Answer Question 10(a) only for the plaintiffs listed below to which you answered "Yes" to any of Questions 1 through 8.]

(i)	Yukos Capital	Yes _____	No <u>X</u>
(ii)	Yukos Hydrocarbons	Yes _____	No <u>X</u>
(iii)	2015 Security Trust	Yes _____	No <u>X</u>

[If your answer to any subpart of Question 10.(a) is "Yes," then you must proceed to Question 10.(b). If your answer to all sub-parts of Question 10.(a) is "No," then you should skip Question 10.(b) and proceed to question 10.(c).]

- (b) Answer this question only for each plaintiff for which you answered "Yes" in Question 10.(a). In the rightmost column titled "Compensation Earned During any Period(s) of Substantial Disloyalty," enter in dollars the amount, if any, that you find, by a preponderance of the evidence, that Mr. Feldman received as compensation based on his service to that particular plaintiff during the period of his substantial disloyalty.

<u>Plaintiff</u>	<u>Compensation Earned During any Period(s) Of Substantial Disloyalty</u>
(i) Yukos Capital	<u>X</u>
(ii) Yukos Hydrocarbons	<u>X</u>
(iii) 2015 Security Trust	<u>X</u>

[Answer Question 10.(b) only for the plaintiffs listed below to which you answered "Yes" to Question 10.(a).]

- (c) Has each plaintiff listed below proved, by a preponderance of the evidence, that Mr. Feldman acted with an evil motive or intent, or with reckless or callous indifference to the plaintiff's rights by engaging in any of the schemes for which you earlier found a breach of fiduciary duty with respect to that plaintiff?

[Answer Question 10.(c) only for the plaintiffs listed below to which you answered

"Yes" to any of Questions 1 through 8.]

(i)	Yukos Capital	Yes _____	No <u>X</u>
(ii)	Yukos Hydrocarbons	Yes _____	No <u>X</u>
(iii)	Foundation I	Yes _____	No <u>X</u>
(iv)	Foundation II	Yes _____	No <u>X</u>
(v)	2015 Security Trust	Yes _____	No <u>X</u>

[Please sign your names in the space provided below and inform the Officer that you have reached a verdict.]

_____	_____
_____	_____
_____	_____
_____	_____
_____	_____

Dated: March , 2019

EXHIBIT

2

**UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK**

-----X
YUKOS CAPITAL S.A.R.L., YUKOS
HYDROCARBONS INVESTMENTS LIMITED,
STICHTING ADMINISTRATIEKANTOOR
YUKOS INTERNATIONAL, STICHTING
ADMINISTRATIEKANTOOR FINANCIAL
PERFORMANCE HOLDINGS, LUXTONA
LIMITED and MARC FLEISCHMAN, TRUSTEE
OF THE 2015 SECURITY TRUST, as successor in
interest to the 2004 SECURITY TRUST,

Plaintiffs,

-against-

DANIEL CALEB FELDMAN,

Defendant.
-----X

DANIEL CALEB FELDMAN,

Counterclaim-Plaintiff,

-against-

YUKOS CAPITAL S.A.R.L., et al.,

Counterclaim-Defendants.
-----X

DANIEL CALEB FELDMAN,

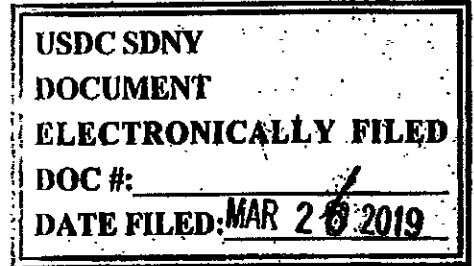
Third-Party Plaintiff,

-against-

DAVID GODFREY, STEVEN THEEDE, MARC
FLEISCHMAN, BRUCE MISAMOR, MICHEL de
GUILLENCHMIDT, GRETCHEN KING,
FINANCIAL PERFORMANCE HOLDINGS B.V.,
FAIR OAKS TRADE AND INVEST LIMITED and
DIRECTORS PROTECTION LTD, SOLELY IN ITS

15-cv-4964 (LAK)

JUDGMENT



CAPACITY AS THE TRUSTEE FOR THE
DIRECTORS PROTECT TRUST,

Third-Party Defendants.

-----X

The case having been tried to verdict by a jury and the Court having resolved many of the claims by interlocutory rulings, it is hereby

ORDERED, ADJUDGED AND DECREED that plaintiffs Yukos Capital S.A.R.L., Yukos Hydrocarbons Investments Limited, Stichting Administratiekantoor Yukos International, Stichting Administratiekantoor Financial Performance Holdings, and Marc Fleischman, as trustee of the 2015 Security Trust, as successor in interest to the 2004 Security Trust, each recover of defendant nominal damages of \$1, and it is further

ORDERED, ADJUDGED AND DECREED that the claims of plaintiff Luxtona Limited against the defendant and all counterclaims, crossclaims, and third party complaints are dismissed.

DATED: New York, New York
March 25, 2019

So Ordered:

U.S.D.J.

RUBY J. KRAJICK

Clerk of Court

BY:

Deputy Clerk

EXHIBIT

3

10:44

FELDMAN23@gmail.com inbox






Rishi



Cancel



All Mailboxes

Current Mailbox

-
- 

Rishi Bhandari 10/10/18 




 Trial Schedule

 Or if you're available now, call my cell.

 917-514-7135. Rishi Bhandari Mandel Bhandar...
-
- 
Rishi Bhandari 10/9/18 



 Trial Date Adjourned

 Trial date was adjourned to March 4, 2019 (with

 no guarantee of trial going forward on that day...
-
- 

Rishi Bhandari 10/5/18 



 Yukos v. Feldman

 Daniel, Just to close the loop on this, is our

 response that Dmitri wired \$500,000 directly t...
-
- 
Daniel Feldman 10/2/18 




 Fwd: wire transfer

 This is what I thought. Sent from my iPhone

 Begin forwarded message:
-
- 
Rishi Bhandari 9/28/18 




 Schedule

 If trial starts that day you can't go to any

 meeting that evening. We need to be able to p...
-
- 

Daniel & Rishi 9/28/18 

 Schedule

 Just tried your office. Sorry the day got away

 from me. Any further thoughts on the schedul...
-
- 

Rishi Bhandari 9/11/18 

 Family Photos

 Actually, we're going to put together a list of

 events that are going to be discussed in your...
-

Edit

10:44

Feldman 23@gmail.com inbox

Q Rishi



Cancel

All Mailboxes

Current Mailbox

**Rishi & Gea**

8/6/18 >

Feldman / advice - new version affidavit [A...



Gea, I've attempted to answer your questions below. If this is not sufficient, let's plan to talk...

**Rishi Bhandari**

8/3/18 >

Revised Declaration and Supporting Invoices



Gea, Thanks again for flagging the discrepancy between what we billed and and what we recei...

**Daniel & Rishi**

8/2/18 >

Indemnification Action

Yes. That works. Sent from my iPhone

**Rishi & Gea**

8/2/18 >

Feldman / Advice - amount of the claim [AMS-...

We should be able to figure this out today. I sent it to my partner who is looking into it. Rishi Bh...

**Rishi Bhandari**

8/1/18 >

Decision on Yukos' Sanction Motion



I'm not sure of what motion, if any, we should file to clarify this issue but we're giving it som...

**Rishi & Gea**

8/1/18 >

Declaration [AMS-15968-20150238]

Gea, I just wanted to make sure there's nothing else you need from me. If there is, please let m...

**Daniel & Rishi**

7/25/18 >

Declaration



...07 AM, Rishi Bhandari

<rb@mandelbhandari.com> wrote: Gea, Apolo...

Edit

10:45

Feldman23@gmail.com inbox






Rishi







Cancel

All Mailboxes



Current Mailbox


-
- 

Rishi Bhandari 1/20/17 



Letter to Yukos re Additional Documents 

 Sorry, I thought this was general enough but, at the same time, provided some justification for...
-
- 

Daniel Feldman 9/22/16 



Notarized Document

 Asking as I have been asked for permission for it to used as an exhibit in Amsterdam. They want...
-
- 
Rishi & Hidde 9/8/16 




Documents Relevant to a Dutch Indemnific... 


 Thank you very much. This is very, very helpful. Let me speak to the party regarding funding a...
-
- 
Rishi Bhandari 9/7/16 



Re: Engagement_letter_AMS_EN Feldman_ Ad...

 Hidde, I hope all is well. I am writing because I have finally gotten some clarity on potential fu...
-
- 
Rishi Bhandari 8/17/16 

Fwd: Email Search

 Daniel, see below. It appears that the email wasn't produced. Should we make a follow up...
-
- 

Rishi Bhandari 8/17/16 

Common interest privileged communication 

 Let's have a conversation. I'm on a plane right now. Scheduled to land in 2 hours. Can we hav...
-
- 
Rishi Bhandari 7/26/16 

Credit Card Information

 Daniel, Thanks for checking to see if you have any credit card statements reflecting travel ex...
-

Edit

11:06



< amended complaint

caleb23@aol.com
inbox

Emails Photos Documents

Category ▾

Sent

Received

Starred



2016

Edit

Sent/caleb23@aol.com



Robert Glunt

1/28/16

Re: Draft Amended Counterclaims

...016 5:02 pm Subject: Draft Amended Count...



Inbox/caleb23@aol.com



Me

1/28/16

Re: Draft Amended Counterclaims

...7:41 pm Subject: Re: Draft Amended Counte...



Sent/caleb23@aol.com



Rishi Bhandari

1/28/16

Re: Draft Amended Counterclaims

...016 5:02 pm Subject: Draft Amended Count...



Inbox/caleb23@aol.com



Me

1/28/16

Re: Draft Amended Counterclaims

...016 5:02 pm Subject: Draft Amended Count...



Sent/caleb23@aol.com



Robert Glunt

1/28/16

Re: Draft Amended Counterclaims

...I - I've attached our draft Amended Counter...



Inbox/caleb23@aol.com



Robert Glunt

1/28/16

Draft Amended Counterclaims

Daniel - I've attached our draft Amended Cou...



Inbox/caleb23@aol.com

11:23



< glunt

Caleb23@aol.com
inbox

Emails Photos Documents

✶ Sent

✉ Received

☆ Starred

• Unread



2016

Edit

Inbox/caleb23@aol.com



Robert Glunt

7/8/16

Re: Transcripts

...ipt attached. Best regards, Rob Glunt On Fri,...



✉ Inbox/caleb23@aol.com



• Rishi Bhandari

7/1/16

Fwd: New documents: Yukos Capital SARL et...

Fyi... ----- Forwarded message ----- Fro...



✉ Inbox/caleb23@aol.com



Me

7/1/16

Re: Transcripts

...iginal Message----- From: Robert Glunt <glun...



✶ Sent/caleb23@aol.com



Robert Glunt

7/1/16

Re: Transcripts

Theede, Godfrey, and Fleischman transcripts...



✉ Inbox/caleb23@aol.com



Me

7/1/16

Transcripts

Rob: Please send me The Theede, Godfrey, Fle...



✶ Sent/caleb23@aol.com



• Robert Glunt

6/24/16

Letter from Yukos Lawyers

...r records. Best regards, Robert Glunt Mande...



✉ Inbox/caleb23@aol.com

11:25



< glunt

Caleb23@aol.com
inboxEmails Photos Documents

Sent

Received

Starred

Unread



2016

Edit



• Robert Glunt

3/10/16

Re: Info re individuals who received defamat...

...nal Message----- From: Robert Glunt <glunt...



Inbox/caleb23@aol.com



• Robert Glunt

3/10/16

Re: Info re individuals who received defamat...

... 10, 2016 at 11:30 AM, Robert Glunt <glunt@...



Inbox/caleb23@aol.com



Me

3/10/16

Re: Info re individuals who received defamato...

-----Original Message----- From: Robert Glunt <...



Sent/caleb23@aol.com



Robert Glunt

3/9/16

Info re individuals who received defamatory s...

... lawyers? Best regards, Robert Glunt Mandel...



Inbox/caleb23@aol.com



Me

2/23/16

Re: Yukos Case - Two Discovery Questions

...inal Message----- From: Robert Glunt <glunt...



Sent/caleb23@aol.com



Robert Glunt

2/23/16

Yukos Case - Two Discovery Questions

...anything. Best regards, Robert Glunt Mande...



Inbox/caleb23@aol.com



Me

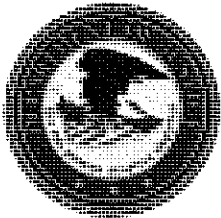
1/31/16

EXHIBIT

4

From: U.S. Department of Justice - VNS fedemail@vns.usdoj.gov
Subject: U.S. Department of Justice - VNS - Investigative Case 2018R00349 -
Court Case 19-CR-00610
Date: Nov 14, 2022 at 2:10:37 PM
To: Daniel Feldman feldman23@gmail.com

DO NOT REPLY TO THIS EMAIL.



U.S. Department of Justice
Southern District of New York
One St. Andrews Plaza
New York, NY 10007
Phone: (212) 637-1028
Fax: (212) 637-0421

November 14, 2022

Daniel Feldman

Re: United States v. Defendant(s) Aviram Azari
Case Number 2018R00349 and Court Docket Number 19-CR-00610

Dear Daniel Feldman:

This notice is provided by the United States Department of Justice Victim Notification System. I am contacting you because you were identified by law enforcement as a victim or potential victim during the investigation of the above criminal case.

There is new information regarding the above referenced matter that can be viewed by accessing the VNS Web page at <https://www.notify.usdoj.gov> and registering with VNS. Registering with VNS provides the ability to access all notifications regarding this case, view any additional documents provided during the case as well as update your personal contact information. You will need the following information to register with VNS: (1) your VNS ID and PIN that was provided to you in the initial email you received from VNS. In addition, if you have received a letter from VNS, your ID and PIN are included in the letter; (2) Your last name or business name as listed in the VNS letter or email.

If you want future email notices from VNS to contain the details regarding the case events, you can elect to "verify" your email address when you register by providing that information during the registration process. Verifying your email with the VNS will also allow you to be assured of receiving timely notifications regarding this matter.

If you do not want to register with VNS, but you want to receive VNS email notices that contain the details about recent events, you should verify your email address by selecting this [link to VNS](#). You will need to provide the following information to verify your email address: VNS ID, your last name or business name, and your email address (you must

enter the same email address used for this message). **Please understand that if you elect to verify your email address without registering with VNS, you will not have access to the VNS Web site.**

If you need assistance with this process, please contact the VNS Help Desk at (866) 625-1631.

Sincerely,

DAMIAN WILLIAMS
United States Attorney

Wendy Olsen
Victim Witness Coordinator

If you do not want to receive email notifications from the Victim Notification System (VNS) please log into the VNS Web site at <https://www.notify.usdoj.gov>, select "My Information", remove your email address and click the "update" button. If you remove your email address, you will continue to receive letters from VNS except in those case which have large numbers of victims. To change your email address, select "My Information", provide a new address and click the "update" button.

If you do not want to receive any notifications in your case, select "Stop Receiving Notifications" and follow the instructions on the screen.

If you believe you have received this email in error, please contact the office listed at top of the email message.

Please note, if this is the first notification you have received from VNS you will need to wait 4-8 hours from receipt of this email before you can login to the VNS Internet site (<https://www.notify.usdoj.gov>). In addition, it will also be 4-8 hours before any documents which may have been uploaded to VNS as part of this notification are available under the "Downloads/Links" section on the Web page.

Please call the Victim Notification System (VNS) Help Desk at phone number [1-866-625-1631](tel:1-866-625-1631) for assistance and questions.

EXHIBIT 5

From: **Shane Crumlish** scrumlish@fbi.gov
Subject: **Azari Case**
Date: **Jul 14, 2022 at 11:50:23 AM**
To: **feldman23@gmail.com**
Cc: **Caroline Ingold** cingold@fbi.gov

Mr. Feldman

My colleague (cc'd) and I are from the FBI New York Cyber division working the Aviram Azari case. We have been informed that you are willing to speak to us about your experience as a victim of hacking activity. Please let me know your availability in the next few weeks and we can set up a meeting.

Regards,
Shane

Special Agent Shane Crumlish
Federal Bureau of Investigation
New York Division
26 Federal Plaza
New York, NY 10278
(212) 384-3520

EXHIBIT 6

#ExxonKnew hacking middleman gets nearly 7 years in prison. We still don't know who hired him.

“Exxon’s silence is deafening,” said one victim of the hacking scheme.

EXXONKNEWS

NOV 17, 2023

Emily Sanders is the Center for Climate Integrity’s editorial lead.

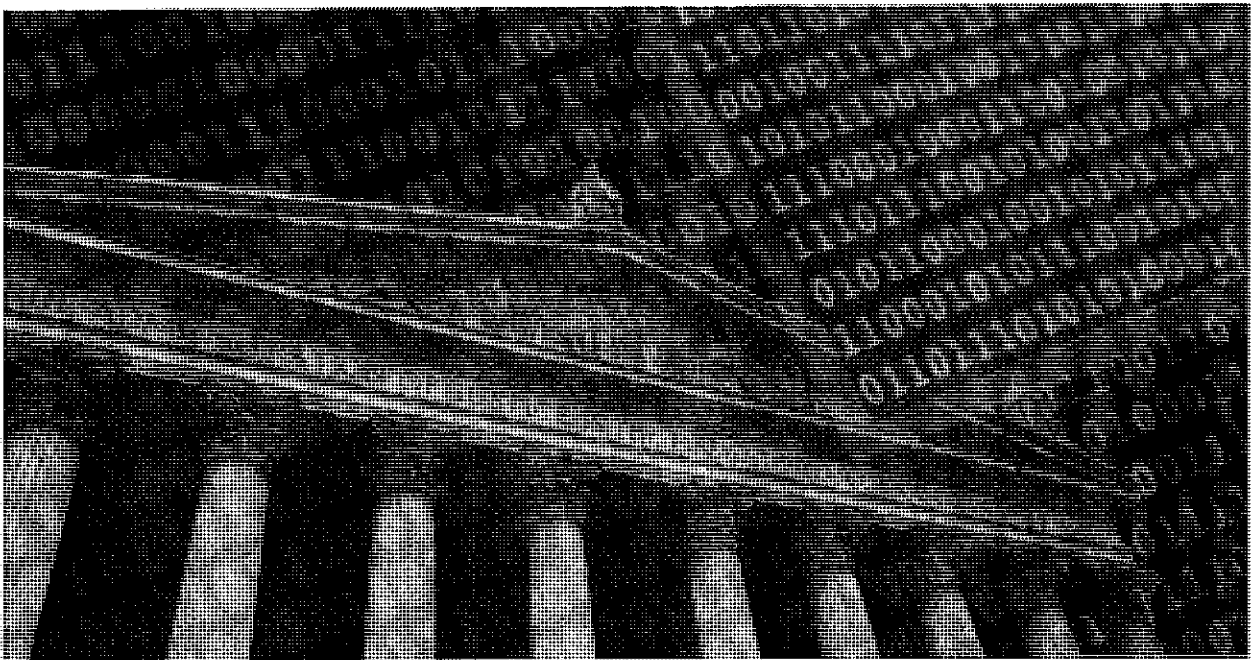


Illustration by Tess Abbot

The man who pleaded guilty to participating in a massive criminal hacking scheme targeting climate advocates who campaigned against ExxonMobil was sentenced to nearly 7 years in prison yesterday, while the question of who hired him remains unanswered.

During his sentencing hearing in federal court in Manhattan, Israeli private investigator Aviram Azari said through a translator that “there will come a day” when he would be able to tell his victims more. Federal prosecutors say Azari

served as the scheme's middleman, connecting his clients with hackers across the globe who were directed to infiltrate the emails and online accounts of thousands of victims and their close friends, family, and coworkers between 2014 and 2019. In 2019, he was arrested on his way to Disneyland and detained in New York.

According to the U.S. Department of Justice, Azari particularly targeted U.S. climate advocates and obtained information that Exxon would later use in court to deflect accusations that the company has engaged in a decades-long campaign to deceive the public about climate change.

"Some of the hacked documents that were stolen from various of the victims' online accounts were leaked to the press, resulting in articles relating to the New York and Massachusetts Attorneys Generals' investigations into Exxon Mobil Corporation's knowledge about climate change and potential misstatements made by Exxon regarding what it knew about the risks of climate change," the DOJ said in a statement yesterday.

Azari had pleaded guilty to counts of wire fraud, conspiracy to commit hacking, and aggravated identity theft last April. None of Azari's clients, who prosecutors say paid Azari \$4.8 million, have been named.

One of the hacking victims, Peter Frumhoff, who was chief climate scientist at the Union of Concerned Scientists until 2021, told *ExxonKnews* after the hearing that the sentencing is hopefully "a stepping stone, not a final moment" of accountability for the illegal attack against key players in the #ExxonKnew movement.

"I would've thought by now, given the facts and circumstances of this case, that the board [of ExxonMobil] would've called for a transparent and independent investigation to make sure that none of their employees or agents were involved in this crime," Lee Wasserman, director of the Rockefeller Family Fund and a victim of the hacking, told reporters outside the courthouse. "But Exxon's silence is deafening."

(Note: ExxonKnews is a project of the Center for Climate Integrity, which is funded in part by grants from the Rockefeller Family Fund. A staff member at the Center for Climate Integrity, Kert Davies, was also a victim of the hacking scheme during his former tenure at the Climate Investigations Center.)



Lee Wasserman, director of the Rockefeller Family Fund, and Miranda Kaiser, president of the Rockefeller Family Fund board of trustees, spoke to the press outside the federal courthouse in Manhattan.

So who could have been behind the hacking of #ExxonKnew activists?

Three victims of the hacking gave statements to the court and asked federal prosecutors to continue their investigation into the hacking scheme.

Frumhoff said that his and other colleagues' emails were hacked at a time when "a great deal of pressure was being brought to bear" on Exxon and other fossil

fuel majors, and that the hacking was a clear attempt to chill their efforts to expose the companies' deception and hold them accountable.

"We have a right to know — the public has a right to know — who [Azari's] clients were," he told the court.

Another victim, Daniel Feldman, who believes he was targeted on behalf of a Russian oligarch living in Israel, spoke directly to Azari during his statement. "You're weak," he told Azari. "If you're truly sorry, you should be giving the names of the people who hired you."

Prosecutors said documents stolen through the hacking scheme were introduced in court filings by Exxon, which argued that advocates had "conspir[ed]" with state attorneys general to unfairly investigate and vilify the company. One private email between lawyers, academics, and advocates about a meeting in January 2016 to develop a plan to publicize Exxon's climate deception was referenced on the company's official #ExxonKnew rebuttal website. But after that email was highlighted in a Wall Street Journal exclusive report as a focus of the Manhattan U.S. attorney's office investigation, the page was promptly taken off the internet.

Wasserman told the courtroom that, at the time he was hacked, his organization was also working to expose Exxon's climate deception. After that meeting in January 2016, Wasserman said he received a call from a reporter who somehow got a copy of the email he and other colleagues had received about the gathering. "It felt like Big Brother had arrived," he said. "I found myself whispering in my own home."

"The extensive targeting of American nonprofits exercising their first amendment rights is exceptionally troubling," reads a 2020 report by Citizen Lab, a University of Toronto cybersecurity research group. Researchers found that the hacking, which included at least one minor child, "increased around certain key events" surrounding Exxon — like the launch of investigations and accountability lawsuits against the company by government officials.

One of those lawsuits, filed by a group of Puerto Rico municipalities, now cites a sentencing memo filed by the U.S. attorney for the Southern District of New York last month, arguing that it "heavily implicates ExxonMobil's participation in the hacking scheme, likely in furtherance and defense of the defendants' racketeering enterprise."

"You don't know everything"

For a case predicated around silence and secrecy, the sounds in the courtroom during the hearing were many: while lawyers and victims addressed the judge, an interpreter muttered Hebrew into a microphone to Azari, who listened to the translations through chunky headphones. Azari himself cleared his throat every few seconds, a likely symptom of a gastro-intestinal illness he developed during his five years in a New York prison which was described at length by his U.S. attorney, Barry Zone. Zone said Azari has been ostracized by prison-mates for "burping incessantly" and punished for seeking medical care, including being left in his cell for 58 hours without food prior to a hospital visit. Azari and his lawyers (one of whom called in from Israel) asked the judge to consider his military service in Israel as a factor, and described the effect of Azari's absence from his wife and daughters.

Prosecutors recommended a prison sentence of up to about 9 years — but the judge, John G. Koeltl, decided on a lesser sentence after taking into consideration the "deplorable" conditions at the Metropolitan Correctional Center where Azari has been held since 2019 and Azari's military service.

Just after the judge handed Azari his sentence, the defendant spoke directly to his victims. "I ask forgiveness — you don't know everything," he said.

ICYMI News Roundup

- [Oil, gas giants could pay climate damage and still profit: research](#)
- [Don't Expect Gas Companies to Pause Business on Gaza's Behalf](#)

EXHIBIT 7

From: **no-reply@usdoj.gov**
Subject: **Welcome to USAfx - Please Register Your Account**
Date: **Oct 11, 2024 at 4:28:22 PM**
To: **feldman23@gmail.com**

An account has been created for you on the DOJ USA File Exchange (USAfx).

To access your account, please click [here](#) and set your password. For security purposes, this link will remain active only for the next 24 hours.

If you have any questions, please contact your sponsor.

- USAfx Administrator

EXHIBIT

8

From: **Murray, Juliana (USANYS) 1** Juliana.Murray@usdoj.gov
Subject: **RE: Daniel Feldman**
Date: **Dec 17, 2024 at 12:19:37 PM**
To: **Daniel Feldman** daniel@buildingblock.io
Cc: **Crumlish, Shane (NY) (FBI)** scrumlish@fbi.gov, **Zverovich, Olga (USANYS)** Olga.Zverovich@usdoj.gov

Mr. Feldman,

I've uploaded the additional documents we identified to USAfx.

Best,
Julie

From: Daniel Feldman <daniel@buildingblock.io>
Sent: Thursday, December 12, 2024 10:36 AM
To: Murray, Juliana (USANYS) 1 <JMurray1@usa.doj.gov>
Cc: Crumlish, Shane (NY) (FBI) <scrumlish@fbi.gov>
Subject: [EXTERNAL] Re: Daniel Feldman

Amazing. Thank you so much.

Sent from my iPhone

On Dec 12, 2024, at 10:11 AM, Murray, Juliana (USANYS) 1 <Juliana.Murray@usdoj.gov> wrote:

Hi Mr. Feldman,

We need to restore our archived database to get these documents. That is in progress, then we'll pull them and get them over to you.

Thank you,
Julie

From: Daniel Feldman <daniel@buildingblock.io>
Sent: Tuesday, December 10, 2024 2:19:01 PM
To: Murray, Juliana (USANYS) 1 <JMurray1@usa.doj.gov>
Cc: Crumlish, Shane (NY) (FBI) <scrumlish@fbi.gov>
Subject: [EXTERNAL] Re: Daniel Feldman

Julie:

Checking in on the below. Hoping you can arrange to have the additional emails added to the portal you set up.

Best

EXHIBIT

9



From: Murray, Juliana (USANYS) 1 Juliana.Murray@usdoj.gov
Subject: RE: Daniel Feldman
Date: December 17, 2024 at 5:31 PM
To: Daniel Feldman daniel@buildingblock.io
Cc: Crumlish, Shane (NY) (FBI) scrumlish@fbi.gov, Zverovich, Olga (USANYS) Olga.Zverovich@usdoj.gov

Hi Mr. Feldman,

This was all we found for dan[@]mondogoal.com. We did not identify any of the invoices you've indicated you're looking for.

The AZ document was an attachment to an email from one of Azari's aliases to another person, the cover email is copied below:

Daniel C. Feldman

Sent: Mon 1/18/2016 1:56:53 PM (UTC)

From: Walter Heisenberg

To: poui kremer



Total between Arshad and Daniel.JPG
170.5 KB

Id's used by Daniel Caleb Feldman:

caleb23@aol.com (The one we got from customer)

dan@mondogoal.com

feldman23@gmail.com

feldmand@yukos.ru

See attached total amount of mails between Daniel C. Feldman to the one we have.

Thank you,
Julie

From: Daniel Feldman <daniel@buildingblock.io>
Sent: Tuesday, December 17, 2024 1:58 PM
To: Murray, Juliana (USANYS) 1 <JMurray1@usa.doj.gov>
Cc: Crumlish, Shane (NY) (FBI) <scrumlish@fbi.gov>; Zverovich, Olga (USANYS) <OZverovich@usa.doj.gov>
Subject: [EXTERNAL] Re: Daniel Feldman

Thank you so much Juliana!

Can you explain what the AZ_00318533 document is?

Sent: Mon 1/18/2016 1:56:53 PM (UTC)

Daniel C. Feldman

From: Walter Heisenberg

To: poul kremer



Total between Arshad and Daniel.JPG
170.5 KB

Id's used by Daniel Caleb Feldman:
caleb22@aol.com (The one we got from customer)
dan@mondogal.com
feldman22@gmail.com
feldmand@yukos.ru

See attached total amount of mails between Daniel C. Feldman to the one we have.

EXHIBIT 10



From: Murray, Juliana (USANYS) 1 Juliana.Murray@usdoj.gov
Subject: RE: Daniel Feldman
Date: January 14, 2025 at 12:34 PM
To: Daniel Feldman daniel@buildingblock.io
Cc: Crumlish, Shane (NY) (FBI) scrumlish@fbi.gov, Zverovich, Olga (USANYS) Olga.Zverovich@usdoj.gov

Mr. Feldman,

With thanks to SA Crumlish, below and attached is additional information.

Evidence reflects that you were added to "Project Yummy" as a new target on March 3, 2017 (AZ_00061410).

AZ_00185612 – Cover email for Invoice 104, 12/01/2016
AZ_00096136 - Cover email for Invoices 107 and 108, 12/29/2016
AZ_00285953 - Cover email for Invoice 117, 3/21/2017
AZ_00252940 - Cover email for Invoice 123, 4/24/2017
AZ_00252995 - Cover email for Invoice 124, 4/24/2017
AZ_00591172 - Cover email for Invoices 116, 117, 123, 124, 129, 130, and 132.
Email sent 10/18/2017, but Azari notes the invoices range from Feb-Sept 2017
AZ_00591738 - Cover email for Invoices 141, 142, 149, and 153. Email sent on 8/28/2018.

EXHIBIT 11

From: **Murray, Juliana (USANYS) 1** Juliana.Murray@usdoj.gov
Subject: **RE: Question**
Date: **Mar 10, 2025 at 2:42:19 PM**
To: **Daniel Feldman** daniel@buildingblock.io, **Crumlish, Shane (NY) (FBI)**
scrumlish@fbi.gov

Hi Mr. Feldman,

Invoices 108 and 153 are attached. We cannot provide an unredacted version of AZ_00061410, but I can confirm that it was sent from one of the Belltrox leaders to one of the Belltrox hackers.

Thank you,
Julie

-----Original Message-----

From: Daniel Feldman <daniel@buildingblock.io>
Sent: Monday, March 10, 2025 11:46 AM
To: Murray, Juliana (USANYS) 1 <JMurray1@usa.doj.gov>; Crumlish, Shane (NY) (FBI) <scrumlish@fbi.gov>
Subject: [EXTERNAL] Re: Question

Following up on the below about document AZ_00061410. Also writing to see if you can provide me with invoices 108 and 153. Both are Nerodia invoices to Vantage Intelligence referenced in emails you provided. You sent me all the other invoices but not those two.

Thank you!
Daniel
Sent from my iPhone

On Mar 4, 2025, at 5:38 PM, Daniel Feldman <daniel@buildingblock.io> wrote:

Juliana and Shane:

I hope you guys are well. I am slowly finishing my appeal brief. I hope to have it completed this weekend.

I have a request about document AZ_00061410, which is an email entitled New

EXHIBIT 12



From: Murray, Juliana (USANYS) 1 Juliana.Murray@usdoj.gov
Subject: RE: Near Final Draft
Date: March 31, 2025 at 10:53 AM
To: Daniel Feldman daniel@buildingblock.io, Crumlish, Shane (NY) (FBI) scrumlish@fbi.gov

Hi Mr. Feldman,

Confirming receipt of all three drafts. I take no stance or position on any substance, but I do not see anything from my read through that is factually inaccurate.

Thank you,
Julie

-----Original Message-----

From: Daniel Feldman <daniel@buildingblock.io>
Sent: Friday, March 28, 2025 12:57 PM
To: Murray, Juliana (USANYS) 1 <Juliana.Murray@usdoj.gov>; Crumlish, Shane (NY) (FBI) <scrumlish@fbi.gov>
Subject: [EXTERNAL] Near Final Draft

Juliana and Shane:

Attached you will find a much improved draft. I plan to file mid-week next week.

Please let me know if you have any feedback. It would be amazing if after reading you think of any additional evidence you can provide that would bolster my motion and help hold these people accountable for their illegal acts. It would also help me clear my name.

You have not responded to the other two drafts. If possible, please acknowledge receipt. I can also be reached at 1-646-703-4350. If you would like to review the exhibits that I have attached, I am happy to bring them to your office. It is too many pages to attach on an email.

I hope you had a good week.

Daniel

EXHIBIT 13

From: "Bing, Christopher (Reuters)" <Christopher.Bing@thomsonreuters.com>
Date: July 7, 2022 at 10:37:20 PM EDT
To: feldman23@gmail.com
Subject: Belltrox - Mercenary Hacking effort on your account. Story now public.

Hello,

My name is Chris Bing, I am an investigative reporter with Reuters focused on cybersecurity and intelligence. If you are getting this email today than it is likely you've already received one of my messages in the past.

A colleague (Raphael Satter) and I have been sending requests for comment via email to targets of an expansive mercenary hacking campaign beginning in 2019: <https://www.reuters.com/article/us-india-cyber-mercenaries-exclusive/exclusive-obscure-indian-cyber-firm-spied-on-politicians-investors-worldwide-idUSKBN23G1GQ>

As you may already know, your email was among those targeted.

The goal of this outreach effort has been to understand why individuals like yourself would have been targeted by these hackers between 2013 and 2020. The hackers themselves often worked on behalf of private investigators, hired by wealthy clients.

Two years later, we have spoken to hundreds of fellow targets and written an initial story about what occurred and who is behind it. The article contains additional information about the data and methodology we used to discovery more details (which may be helpful to you).

Story is here – published late last week: <https://www.reuters.com/investigates/special-report/usa-hackers-litigation/>

In summary, the article explains that this mercenary hacking activity was often designed to steal documents or information relevant to different litigation battles around the globe.

While we've spoken to many of you already, some remain that haven't responded or who may be unaware of the final article.

If you've already responded to our email outreach or simply do not want to speak with me then please feel free to ignore my message. However, if you're familiar with this topic or feel that you may have useful information to share then please get in touch.

The easiest way to reach me is through this email.

Here's some additional background about me (the twitter account will validate this email address is authentic):

- <https://www.linkedin.com/in/232958356/>
- https://twitter.com/Bing_Chris
- <https://bing-chris.medium.com/how-to-contact-me-d2fd4bd3ed7b>

Thank you for your help. Take care.

Respectfully,

-Chris Bing

EXHIBIT 14

A REUTERS SPECIAL REPORT

How mercenary hackers sway litigation battles

SPY PHISHING: Hackers based in India attempted to obtain the emails of lawyers and litigants in legal cases across the globe, Reuters found. Illustration by REUTERS/John Emerson.
Photo REUTERS/Raphael Satter

A trove of thousands of email records uncovered by Reuters reveals Indian cyber mercenaries hacking parties involved in lawsuits around the world – showing how hired spies have become the secret weapon of litigants seeking an edge.

By [RAPHAEL SATTER](#) and [CHRISTOPHER BING](#) |

Bodyguard Carlo Pacileo was under mounting pressure. His boss, a direct sales entrepreneur named Ryan Blair, wanted compromising material against a business rival amid a flurry of lawsuits, Pacileo said. Nothing was turning up.

So he turned to a Silicon Valley detective he knew from his days in Afghanistan with the U.S. mercenary firm Blackwater. Nathan Moser, a former North Carolina sheriff's deputy, arrived days later at Pacileo's Hollywood apartment with a duffel bag full of surveillance equipment.

Moser showed Pacileo several gadgets, including Israeli-made listening devices that could be hidden in ceilings or behind television sets. One particular service stood out: Moser said he knew an Indian hacker who could break into emails. "My ears perked up," Pacileo told Reuters recently. "I didn't know you could do that type of stuff."

Moser, who confirmed Pacileo's account, got the job and a \$10,000 per month retainer. He went to work for Blair's company, diet shake distributor ViSalus, as it filed a series of lawsuits against sellers who had jumped ship to go with a competitor named Ocean Avenue.

Starting around February 2013, the Indian hacker – a young computer security expert named Sumit Gupta – broke into the email accounts of Ocean Avenue executives, sending screenshots and passwords back to his ViSalus handlers on the West Coast.

When Ocean Avenue learned of the spying, it filed a federal lawsuit against ViSalus in Utah alleging extortion, intimidation and hacking. ViSalus initially argued that its competitor had not provided enough evidence to back its claims; it later settled the suit on undisclosed terms.

ViSalus executives did not return messages seeking comment. Messages Reuters sent to Blair, who wasn't named as a defendant in the suit, were marked as "seen" but went unanswered. He did not respond to certified letters sent to his business and home in Los Angeles.

The settlement didn't end the matter. The Federal Bureau of Investigation learned of the hacking and, in February 2015, agents raided Pacileo's and Moser's homes. Both eventually pleaded guilty to computer crimes connected to the Ocean Avenue intrusions.

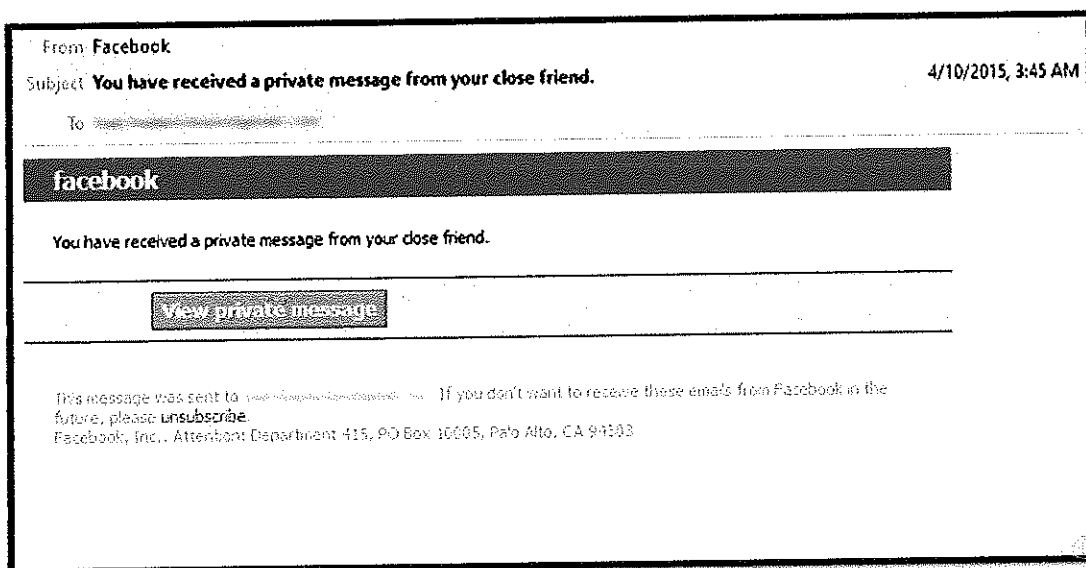
The convictions torpedoed Pacileo's security career and ended Moser's investigation business.

For Gupta it was just the beginning. Over the next decade, he and a small coterie of Indian colleagues built an underground hacking operation that would become a hub for private investigators, like Moser, who sought an advantage for clients embroiled in lawsuits.

Gupta, also charged with hacking in the California criminal case, was never apprehended by U.S. authorities. Reuters has not been able to reach him since 2020, when he told the news agency that while he did work for private investigators, "I have not done all these attacks." Recent attempts to speak with or locate him were unsuccessful.

Reuters identified 35 legal cases since 2013 in which Indian hackers attempted to obtain documents from one side or another of a courtroom battle by sending them password-stealing emails.

The messages were often camouflaged as innocuous communications from clients, colleagues, friends or family. They were aimed at giving the hackers access to targets' inboxes and, ultimately, private or attorney-client privileged information.



PHISHY 'FRIEND': A password-stealing email sent by Indian hackers masquerading as Facebook. Identifying details have been blurred./REUTERS research

At least 75 U.S. and European companies, three dozen advocacy and media groups and numerous Western business executives were the subjects of these hacking attempts, Reuters found.

The Reuters report is based on interviews with victims, researchers, investigators, former U.S. government officials, lawyers and hackers, plus a review of court records from seven countries. It also draws on a unique database of more than 80,000 emails sent by Indian hackers to 13,000 targets over a seven-year period. The database is effectively the hackers' hit list, and it reveals a down-to-the-second look at who the cyber mercenaries sent phishing emails to between 2013 and 2020.

The data comes from two providers of email services the spies used to execute their espionage campaigns. The providers gave the news agency access to the material after it inquired about the hackers' use of their services; they offered the sensitive data on condition of anonymity.

Reuters then vetted the authenticity of the email data with six sets of experts. Scylla Intel, a boutique cyber investigations firm, analyzed the emails, as did researchers from British defense contractor BAE, U.S. cybersecurity firm Mandiant, and technology companies

Intel, Microsoft and Google.

Each firm independently confirmed the database showed Indian hacking-for-hire activity by comparing it against data they had previously gathered about the hackers' techniques. Three of the teams, at Mandiant, Google and LinkedIn, provided a closer analysis, finding the spying was linked to three Indian companies – one that Gupta founded, one that used to employ him and one he collaborated with.

"We assess with high confidence that this data set represents a good picture of the ongoing operations of Indian hack-for-hire firms," said Shane Huntley, head of Google's cyber threat analysis team.

Reuters reached out to every person in the database – sending requests for comment to each email address – and spoke to more than 250 individuals. Most of the respondents said the attempted hacks revealed in the email database occurred either ahead of anticipated lawsuits or as litigation was under way.

The targets' lawyers were often hit, too. The Indian hackers tried to break into the inboxes of some 1,000 attorneys at 108 different law firms, Reuters found.

Among the law firms targeted were global practices, including U.S.-based Baker McKenzie, Cooley and Cleary Gottlieb. Major European firms, including London's Clyde & Co. and Geneva-based arbitration specialist LALIVE, were also hit. In 2018, the Indian hackers tried to compromise more than 80 different inboxes at Paris-based Bredin Prat alone.

Cleary declined comment. The five other law firms did not return messages.

"It is an open secret that there are some private investigators who use Indian hacker groups to target opposition in litigation battles," said Anthony Upward, managing director of Cognition Intelligence, a UK-based countersurveillance firm.

The legal cases identified by Reuters varied in profile and importance. Some involved obscure personal disputes. Others featured multinational companies with fortunes at stake.

From London to Lagos, at least 11 separate groups of victims had their emails leaked publicly or suddenly entered into evidence in the middle of their trials. In several cases, stolen documents shaped the verdict, court records show.

"It is an open secret that there are some private investigators who use Indian hacker groups to target opposition in litigation battles."

Anthony Upward, managing director of Cognition Intelligence, a UK-based countersurveillance firm

Aspects of Gupta's operation have been reported on previously by Reuters, other media and cybersecurity researchers. But the breadth of his involvement in legal cases – and the role of a wider network of Indian hackers – are being reported here for the first time.

The FBI has been investigating the Indian hacking spree since at least early 2018 to determine who, beyond Moser, hired Gupta's crew to go after American targets, according to three people briefed on the matter. The FBI declined to comment.

The email trove provides a startling look at how lawyers and their clients are targeted by cyber mercenaries, but it leaves some questions unanswered. The list doesn't show who hired the spies, for example, and it wasn't always clear whether the hacking was successful or, if so, how the stolen information was used.

Still, Google's Huntley said the attempts to steal privileged information were troubling. "These attacks have real potential to undermine the legal process."

How the Hackers Tried to Fool Lawyers and Steal Their Emails

HACKER HIT LIST: This is an edited version of the data reviewed by Reuters which shows how Indian mercenary hackers hunted lawyers' inboxes. The far left hand column shows when malicious emails were sent; the left hand column shows who the emails were

Forbes issues top 10 powerful Lawyers of US

Lawyers Who Lead by Example

LALIVE counsel named as best woman lawyer in Europe

Time Traveling is possible Now: American Scientists Have Simulated Time Travel With Ph

Ex Al-Qaeda Member Claims ISIS Created & Funded by CIA

Hollywood's Scarlett Johansson Latest LEAKED Sex Scandal

You have a pending incoming docs shared with you from @lalive.ch

Willkommen Sie zu unserem Youporn-Service

Willkommen Sie zu unserem Youporn-Service

Wall Street Journal asking about impact of logistics solutions in Law practice

You have been successfully subscribed to Youporn.com

Your daily love dose Youporn | Adam for Adam !!!

Delivery Status Notification (Failure)

Message left on server: "Undelivered: Claim # 8054711 - Wind Damage"

We've received a report abuse for your LinkedIn account

Please find attached the required documents.

m> Mail Failure Notice

m> Mail Failure Notice

in 2013 and has since launched several tech startups in India.

Goyal said repeat customers comprised much of BellTroX's income. "In this industry, genuine work comes only from recommendations," Goyal said. Reuters was unable to determine the total annual revenue of Gupta's firm.

Before launching BellTroX, Gupta had worked for Appin, an Indian company that initially made its name in cybersecurity training franchises and mainstream IT security work.

By 2010 a division of Appin began hacking targets on behalf of governments and corporate clients, according to six ex-employees, a former U.S. intelligence official, private detectives and Appin surveillance proposals seen by Reuters.

Matthias Willenbrink, a German private investigator and former president of the World Association of Detectives, said he received one such spy proposal from Appin around that time.

Willenbrink said he would not normally use hackers and worked with Appin only once, amid a high-stakes inheritance dispute in 2012 for a wealthy German businessman. The client, who Willenbrink declined to name, wanted to know who was trying to blackmail him anonymously.



HACKER HELP: Matthias Willenbrink turned to a hacker to unmask an alleged blackmailer of his client. REUTERS/Annegret Hilse

Willenbrink was tasked with identifying the culprit. He said he paid Appin about \$3,000 to successfully get into the target's email account. "I was deeply impressed," said Willenbrink, who solved the case. "They sent me all their communications in three days."

The Indian hackers were recruited in big name lawsuits too.

Around the time that Willenbrink was hunting the blackmailer, Israeli private detective Aviram Halevi hired Appin for a "considerable amount" to hack a Korean businessman amid a legal dispute over the rights to distribute KIA Corp cars in Israel, according to a court ruling issued last year in Tel Aviv.

The judge overseeing the case ordered Halevi to pay compensation and destroy the hacked data. Halevi, who admitted to hiring the Indian hackers in an affidavit, declined to comment. A KIA spokesperson also declined to discuss the case. An attorney for the Korean victim didn't return emails.

Several India-based cyber defense training outfits still use the Appin name – the legacy of a previous franchise model – but there's no suggestion those firms are involved in hacking. Appin itself largely disappeared from the internet after the publication of a 2013 cybersecurity research report which connected it to alleged hacking.

Rajat Khare, Appin's co-founder and the former head of several Appin companies, including the Appin Security Group, did not respond to messages seeking an interview. His attorney denied any wrongdoing and said Khare "will not comment on a company he left ten or so years ago."

As Appin's reputation grew, so did its competition. Gupta was part of a cohort of Appin alumni who left the firm around 2012 to found similar companies.

"If you want this information, I can get it."

Hacker Sumit Gupta to private detective Nathan Moser, according to Moser.

Another Indian spy firm registered within a few months of BellTroX was CyberRoot Risk Advisory Private Ltd, based in the Delhi suburb of Gurugram, two former employees and two private investigators familiar with the matter told Reuters.

Appin, BellTroX and CyberRoot have shared computer infrastructure and staff, according to court records and cybersecurity researchers. LinkedIn, Google and Mandiant researchers who reviewed Reuters' data said it shows a mix of hacking activity linked to the companies between 2013 and 2020.

CyberRoot has not responded to messages seeking comment. There was no trace of CyberRoot or BellTroX at the addresses listed for the firms when a Reuters reporter visited recently. Neighbors said they were unfamiliar with the companies.

When Reuters contacted Gupta two years ago, he denied wrongdoing. He was no spy, he said, although he acknowledged he helped private detectives with their IT. "It's not a big deal to provide them a little technical support," he said. "Downloading mailboxes can be a part of it."

In 2017, one of those mailboxes found its way into a \$1.5 billion international legal battle.

Hacking the 'real truth'

That June 11, an explosive email landed in the inbox of international arbitrators weighing the fate of lucrative Nigerian oil fields.

The message, entitled "The real truth about Pan Ocean Oil vs Nigeria," seemed to torpedo the Nigerian government's case in a lawsuit that pitted it against the heirs of Italian businessman Vittorio Fabbri over control of the Pan Ocean Oil Corporation Ltd.

Fabbri had bought the company in 1983, allowing him to pump crude oil in a block of Niger Delta fields known as OML-98. A power struggle later saw him frozen out of the company in favor of local management. After he died in 1998, his heirs fought to regain control, eventually accusing government officials of supporting efforts to oust them.



HACKING LITIGATION: A phony email complicated a legal fight in Nigeria over the Pan Ocean Oil Corp. REUTERS/Tife Owolabi

In 2013 the Fabbri took the fight to the Washington-based International Centre for Settlement of Investment Disputes, which arbitrates legal fights between investors and governments. Patrizio Fabbri, Vittorio's son, told Reuters it was a bid to pull the litigation out of slow-moving Nigerian courts and extract \$1.5 billion in compensation.

The mysterious June 11 email appeared to promise victory for the Fabbri side. Attached were documents from Nigeria's legal team addressed to the managing director of Pan Ocean, asking him to reimburse the government's legal fees. "I wish to remind you of the outstanding fees due to my firm," one of the documents said, requesting that "a sizeable portion" be "paid immediately."

The Fabbri saw the request as a key admission because their case hinged on proving that Pan Ocean and the Nigerian government had colluded to deny the family control of the company.

Bizarrely, the email appeared to have been sent to the arbitrators by Oluwasina Ogungbade, an attorney for the Nigerian government. The lawyer seemed to be sabotaging his client's case. Patrizio said he was thrilled to learn of the apparent admission.

"Wow," he recalled thinking. "Finally somebody in Nigeria is honest."

In interviews with Reuters, Ogungbade declined to address the documents' authenticity but did say he never sent them to the tribunal. Instead, he said, hackers stole the documents, created a fake email in his name and used it to send the material to the arbitrators.

An October 2017 Nigerian police report reviewed by Reuters backs his account, saying, "there is a strong suspicion that some unknown suspect(s) were the authors" of the message.

Pan Ocean and Nigerian officials did not respond to messages seeking comment.

The Indian hacking records reviewed by Reuters fill the gaps in the story.

Gupta's BellTroX made repeated attempts to hack Ogungbade's account. Also targeted were more than 100 employees of Pan Ocean and other lawyers for the Nigerian government, according to the Indian hit list and other data gathered by cybersecurity researchers.

Shortly after, BellTroX created a WikiLeaks-style website titled Nigeriaoilleaks.com, promising to expose corrupt Nigerian politicians and sharing a larger cache of stolen Pan Ocean emails for download.

Over Ogungbade's objections, the tribunal accepted the files sent under his name, although it warned that it "may decide to give the documents little or no weight" if their provenance remained in doubt.

In 2020 the tribunal ruled against the Fabbri family, finding that the government wasn't a party to the takeover; the stolen emails were barely mentioned in the judgment.

Still, Ogungbade believes the leaks convinced arbitrators to deny the Nigerian government most of its legal costs. While Reuters couldn't independently verify that claim, the government was awarded just \$660,000 of the \$3.8 million it had sought.

Reuters wasn't able to learn who commissioned the hack. Patrizio Fabbri said he had "nothing to do" with it. His family's Nigerian lawyer, Olanpo Shasore, said he and colleagues were "all confounded" by their sudden stroke of luck.

Such high-stakes court cases can feature multiple third parties, including litigation financiers, with an interest in the outcome. Two of the tribunal's arbitrators – Boston University professor William Park and arbitrator Julian Lew – did not respond when contacted by Reuters. The third, former Kenyan High Court judge Edward Torgbor, declined comment.

Torgbor had aired concerns about the leak, however. In a 2018 minority opinion he warned that accepting documents of "dubious character" posed a "grave risk" to the tribunal's integrity. "How does the Tribunal discover or uncover the 'real truth' from an unknown person whose own identity and probity are under cover?"

As India's mercenary hacking industry grows, lawyers around the globe are increasingly grappling with similar questions.

WeWork, Wirecard

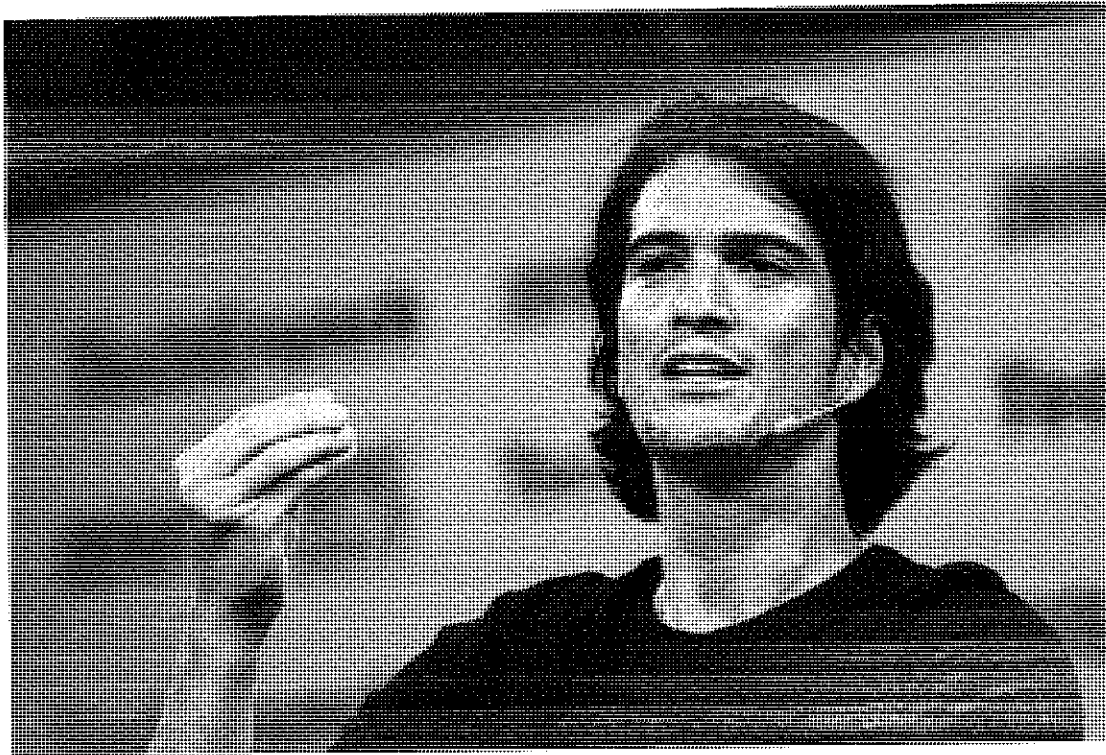
As Reuters contacted victims of the Indian spy campaign, targets involved in at least seven different lawsuits have each launched their own inquiries.

One of the most prominent was WeWork co-founder Adam Neumann, who hired New York's Seiden Law Group after learning from Reuters that he and other company executives' email accounts were targeted by the Indian hackers starting in August 2017, according to four people familiar with the matter.

The hacking attempts against Neumann unfolded as WeWork prepared to announce a \$4.4 billion investment from Japan's SoftBank, a giant infusion for a startup then burning through capital.

By the time Neumann learned of the hacking in 2020, the partnership had collapsed and he was suing SoftBank after being ousted from WeWork. SoftBank executives were quizzed by Neumann's lawyers about the hacking in depositions just weeks before he received a roughly \$500 million settlement from the Japanese investment giant, according to four people familiar with the matter. The executives denied any knowledge of the spying, the sources said.

Reuters was unable to determine who hired the Indian hackers to spy on Neumann or his colleagues. Representatives for Neumann and SoftBank did not return messages. WeWork said the hacking attempts were blocked but did not elaborate. The Seiden Law Group confirmed it had been hired by Neumann to investigate a cybersecurity issue; it declined further comment.



INVESTIGATED HACKS: Adam Neumann, former CEO of WeWork, hired a law firm after learning from Reuters that spies had targeted his emails and those of his coworkers. REUTERS/Eduardo Munoz

Private eyes alleged to have worked as middlemen between their clients and the Indian hackers are coming under increased pressure as victims and law enforcement push for answers.

One of them is former Israeli policeman Aviram Azari, who was arrested by the FBI in 2019. He recently pleaded guilty in New York to wire fraud, identity theft and hacking-related charges after hiring Indian spies to target “a large number” of people, including New York hedge fund employees, prosecutors said in a court filing.

Authorities have released few other details about Azari’s scheme, but four people familiar with the matter say he hired BellTroX to carry out the hacking. Azari’s lawyer, Barry Zone, told Reuters in April that the private eye was prosecuted in relation to his work for the now-defunct German financial firm Wirecard. Zone has not responded to follow-up emails.

Former Wirecard boss Markus Braun was arrested in June 2020 following revelations that 1.9 billion euros were missing from the company’s accounts. The firm collapsed shortly thereafter.

Braun’s legal team declined to comment on Wirecard’s relationship with Azari or BellTroX. Braun has been accused of fraud and market manipulation, charges he denies. His trial is ongoing. Five lawyers for other former top Wirecard executives didn’t return messages.

The hit list seen by Reuters shows BellTroX heavily targeted short sellers, reporters and financial analysts who had voiced skepticism of Wirecard’s business practices before it went bust. In several instances, these hacks coincided with legal threats made by Wirecard.

Azari had other customers, U.S. prosecutors alleged in their filing, saying the Israeli also worked on behalf of numerous undisclosed American clients. “There are thousands of potential victims,” the filing notes. Azari is due to be sentenced later this year, when he faces a prison term of at least two years plus expulsion from the country, prosecutors have said.

Yet the publicity around Azari’s arrest has not deterred India’s mercenary hacking industry. As recently as December, security researchers at Facebook said BellTroX-linked spies were still trying to penetrate the private files of unidentified attorneys across the world.

Jonas Rey, whose Geneva-based company Athena Intelligence is investigating Indian hacks on behalf of several victims, believes some officials in Delhi turn a blind eye to the country’s hack-for-hire market.

Asked about the hacker-for-hire industry, an official with India’s Ministry of Justice referred Reuters to a cybercrime hotline, which did not respond to a request for comment. Delhi police did not return repeated messages seeking comment on Gupta or his hacking business.

He remains a fugitive from U.S. justice. ViSalus, the company that Gupta worked for in 2013, is currently challenging an up to \$925 million class action judgment for placing unsolicited robocalls. Ryan Blair, ViSalus’ CEO, left the firm in 2016.

Blair’s former director of security, Carlo Pacileo, now runs a fitness retreat deep in the mountains of Japan’s Shikoku Island. Nathan Moser, the former private eye, is working on his mental health at a Utah rehabilitation facility following his time in Iraq and Afghanistan.

Reflecting on the Gupta episode recently, Moser said private eyes face immense pressure because they work in “a results-based industry.”

“Hacking is the easiest way to get results,” he said.

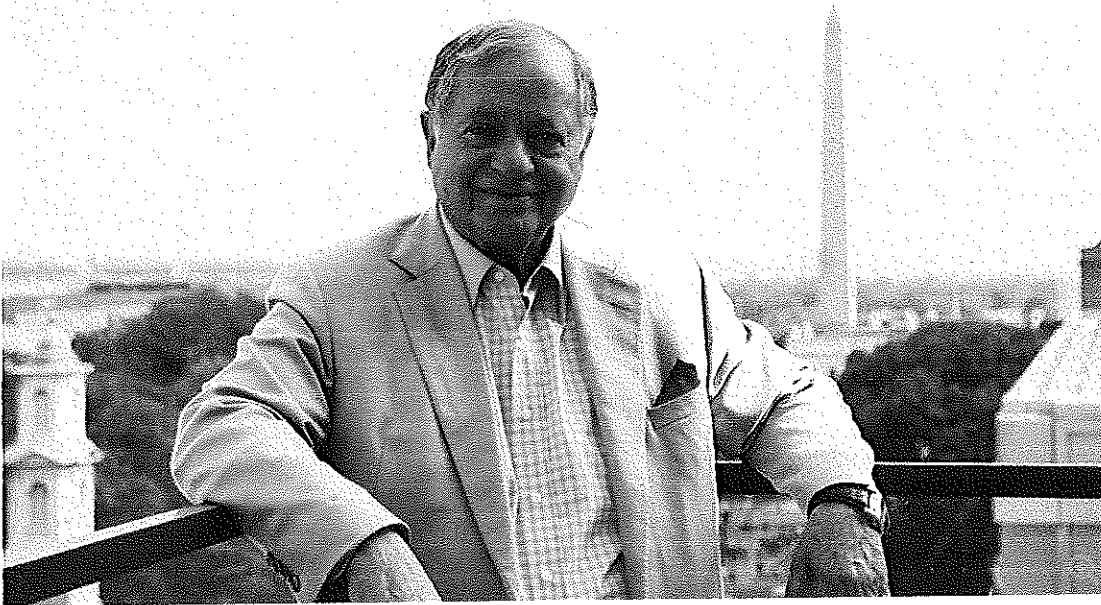
.....

His emails were stolen; now he’s exposing the hack-and-leak industry

By RAPHAEL SATTER and CHRISTOPHER BING

Indian mercenary hackers have worked in the shadows for at least a decade, helping private detectives get an edge in litigation, a Reuters investigation found. Now one victim – an aviation executive named Farhad Azima – is exposing the secretive industry, with potential ripple effects for legal battles on both sides of the Atlantic.

The outlook for Azima once looked grim. In 2020 a judge in London found the Iranian-American liable for cheating his former business partner, an investment fund based in the emirate of Ras Al Khaimah. In a ruling, Judge Andrew Lenon said Azima had been guilty of “seriously fraudulent conduct” in relation to a pair of aviation and tourism-related business deals.



FIGHTING BACK: Aviation executive Farhad Azima said U.S. law enforcement should do more to stop hackers seeking to obtain emails of lawyers and litigants. REUTERS/Raphael Satter

But the case relied heavily on hacked emails that had mysteriously been posted to the web by an apparent whistleblower. Azima – who has long denied the fraud allegations – believed that allies of Ras Al Khaimah’s ruler, Sheikh Saud bin Saqr al-Qasimi, had masterminded the leak in a bid to win at trial.

Witnesses called by the investment fund, known as RAKIA, did nothing to convince him otherwise.

Azima told Reuters he shook his head in disbelief after Israeli journalist Majdi Halabi told the judge he innocently discovered the stolen material “in one of my regular Google searches” for the tycoon’s name in 2016.

Halabi testified that he sent web links to the material to an old friend, British private investigator Stuart Page, who was working for Sheikh Saud and who had asked Halabi to keep an eye out for any Azima-related news. But when cross-examined, Halabi struggled to recall how often he had searched Google for Azima’s name or explain why Page had given him such a peculiar task. Even the judge seemed baffled.

“Presumably Mr Page could have carried out Google searches himself?” Lenon asked.

“The hack-for-hire companies may be thousands of miles away, but the victims are often U.S. citizens on U.S. soil.”

Farhad Azima, who aims to expose the industry that hacked him.

In his May 2020 judgment, Lenon found Halabi's testimony "not credible" and Page's account of how he passed Halabi's information to Sheikh Saud's allies "both internally inconsistent and at odds with the contemporary documents." The judge ruled there was no doubt a hack-and-leak took place and said the explanations provided by RAKIA's witnesses for how they found the documents were full of "unexplained contradictions."

Nevertheless, Lenon said Azima had failed to provide sufficient evidence that RAKIA had hacked his messages. He refused to throw out the emails and ordered him to pay \$4.2 million in restitution.

Hit list

As the ruling was being prepared, Reuters began sifting through a database of more than 80,000 emails Indian hackers had sent between 2013 and 2020. Obtained exclusively by Reuters, the file provides a down-to-the-second look at who the cyber mercenaries targeted in legal battles around the world. It's effectively a hit list. Azima featured prominently.

The Indian hackers had aggressively tried to break into the businessman's emails starting in March 2015. Accounts belonging to Azima's associates, lawyers and friends were also pursued, the records show.

After being contacted by Reuters seeking comment, Azima launched his own inquiry. His legal team combed his inbox and those of his associates, finding more than 700 malicious emails sent over a 16-month period alone. Azima's legal team said his data was breached around March 2016.

In subsequent legal filings, Azima's lawyers accused Indian tech firms CyberRoot Risk Advisory Private Ltd and BellTroX Infotech Services Private Ltd of being behind the espionage campaign.

CyberRoot's hackers created anonymous websites to disseminate Azima's stolen emails using blogs titled "Farhad Azima Scammer" and "Farhad Azima Exposed Again," the court records allege. It was one of those sites that Halabi said he innocently stumbled across in August of 2016.



Farhad Azima | Farhad Azima Scammer

f in t @

Farhad Azima CEO of Aviation Leasing Group- A big Panama Scammer exposed again

Menu

<https://www.mcmonic.com/user/cec8205b-484f-4896-be5b-68b5729daeb9/id/1FBnW>

<https://www.mcmonic.com/user/cec8205b-484f-4896-be5b-68b5729daeb9/id/1FBnW>

#farhad azima #farhad azima exposed
#farhad azima family #farhad azima fraud

Farhad Azima's Devices Data Leaked

Click below to know more about it
<http://www.secdopeer.eu/details/11694381/Farhad-Azima's-Devices-Data-leaked.html>
<http://1337x.to/torrent/1777619/Farhad-Azima-s-Devices-Data-leaked/>

#farhad azima exposed

Farhad Azima Exposed Again

Farhad Azima- An Iranian-born KC aviation figure with colorful past

Tuesday, September 20, 2016

Scams that shamed US

To read in detail click the links:

<http://1337x.to/torrent/1777619/Farhad-Azima-s-Devices-Data-leaked/>
<http://www.secdopeer.eu/details/11694381/Farhad-Azima's-Devices-Data-leaked.html>

Posted by crimelord at 3:14 AM 5 comments **MDL**

Labels: farhad azima exposed, farhad azima family, farhad azima fraud, farhad azima kansas, farhad azima panama papers, farhad azima scam, farhad azima scammer, farhad azima usa

Tuesday, September 13, 2016

Farhad Azima Device Data Leaked

Click the link and find more details:

<http://1337x.to/torrent/1777619/Farhad-Azima-s-Devices-Data-leaked/>
<http://www.secdopeer.eu/details/11694381/Farhad-Azima's-Devices-Data-leaked.html>

Posted by crimelord at 12:50 AM 4 comments **MDL**

Labels: farhad azima exposed, farhad azima family, farhad azima fraud, farhad azima kansas, farhad azima scam, farhad azima scammer, farhad azima usa

Friday, September 9, 2016

Farhad Azima done fraud again

Farhad Azima done fraud again. Download torrent for data:

<http://www.secdopeer.eu/details/11694381/Farhad-Azima's-Devices-Data-leaked.html>

About Me

crimelord

View my complete profile

Farhad Azima

▼ 2016 (9)

► August (4)

▼ September (5)

OMG! Farhad Azima Secrets Revealed
<http://www.bookmark4you.com/tag/farhad-azima-scammer>
Farhad Azima done fraud again
Farhad Azima Device Data Leaked
Scams that shamed US

HACKS, LEAKS & LIES: Hackers have set up WikiLeaks-style websites to distribute stolen emails. These involve aviation executive Farhad Azima, who strongly denies the allegations./REUTERS research

Bank records submitted by Azima's legal team show that CyberRoot was paid more than \$1 million by Nicholas Del Rosso, a London cop-turned-North Carolina private investigator who was working for RAKIA's U.S. law firm, Dechert, at the time of the hack.

A former CyberRoot employee was quoted in one of the filings as saying the "Azima Exposed" sites were intended "to mimic a genuine whistleblower campaign in similar fashion to offshore leaks like the Panama Papers."

Azima successfully won a retrial of his London case, with a three-judge panel at Britain's Court of Appeal ruling in March of last year that the revelations out of India would require "a complete re-evaluation of the evidence in support of the hacking claim."

The businessman added Dechert and one of its former partners as defendants in the ongoing case, alleging the Philadelphia-based law firm and one of its most senior British lawyers, Neil Gerrard, masterminded the hacking operation.

Among Azima's allegations against Gerrard: That he threatened to make him "collateral damage" in the weeks before the leak and that he tried to cover up the hacking by coaching witnesses and laying a false paper trail.

Several legal experts say the suit against Dechert and Gerrard, which is expected to go to trial in 2024, is extraordinary.

"It's unheard of," said David Butler, a partner who heads the civil fraud division at London-based Fox Williams law firm. "I've never known a case where a lawyer is alleged to have commissioned a hack."

Dechert and Gerrard – who has since retired – have denied the allegations and are fighting them in court. Del Rosso did not return messages. In a court filing, he acknowledged paying CyberRoot but said the money was only for routine IT work – not hacking.

CyberRoot and BellTroX did not respond to interview requests. Sheikh Saud's office and RAKIA – now part of the Ras Al Khaimah Economic Zone – did not return messages seeking comment.

Some of RAKIA's original witnesses have since changed their stories.

Stuart Page, the British private eye, now admits in an affidavit he told lies about the way the emails were obtained. Majdi Halabi, the Israeli journalist, has also admitted not telling the truth.

The tale of finding Azima's data through a routine Google search was a "cover story" created to hide the emails' true provenance, Halabi said in an affidavit submitted in February. "I apologise for the false testimony I provided," he added.

Late this month, RAKIA tried to pull out of the case. In a letter to the High Court sent on June 22 and reviewed by Reuters, RAKIA said it had split with its lawyers and was no longer fighting Azima's claim, offering the executive "\$1 million plus costs" to settle the matter. The investment agency said it "did not authorise or procure any hacking of Mr. Azima's data" but added that it may have been the victim of unspecified "dishonest and unscrupulous third party advisers."

Azima's lawyer, Dominic Holden, did not disclose whether the tycoon would accept the offer, saying only that the settlement "will have to reflect the scope and gravity of the wrongdoing."

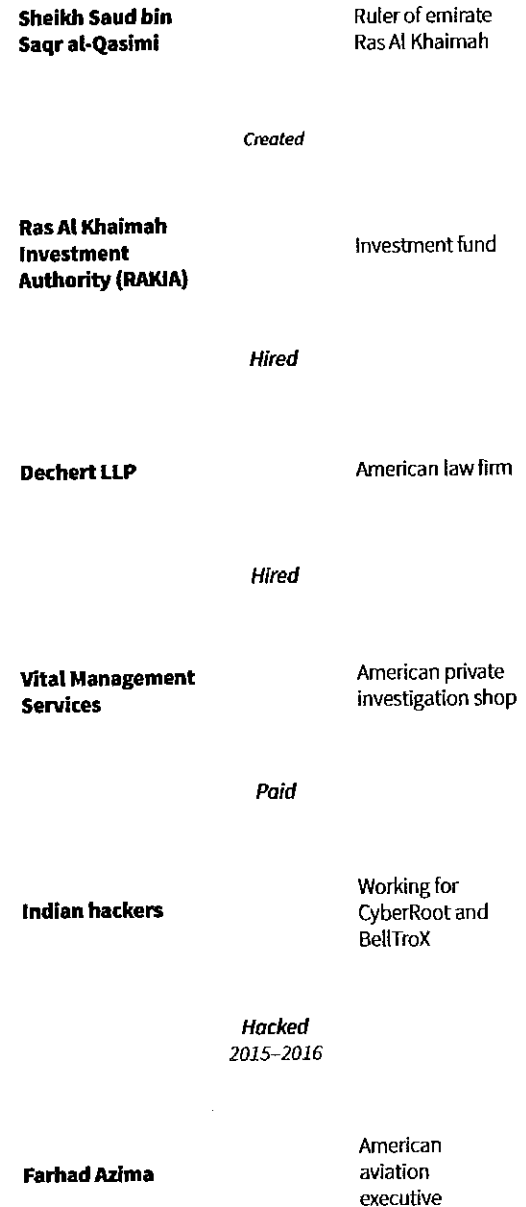
The case's dramatic turnaround is getting attention. Azima spokesman Tim Maltin said at least five other lawyers and businessmen have been in contact with Azima's legal team over suspicions that they too were targeted by Indian hackers as part of separate court battles.

In an email from his home in Missouri, Azima told Reuters American law enforcement needed to do more to stop hackers from targeting litigants.

"Millions of dollars are being made by hackers, investigators and their instructing law firms from these illegal activities," he said. "The hack-for-hire companies may be thousands of miles away, but the victims are often U.S. citizens on U.S. soil."

Following the Money

This chart shows the alleged flow of funds from RAKIA, an Emirati investment agency established by Sheikh Saud bin Saqr al-Qasimi, to its U.S. law firm, Dechert, and to a private intelligence subcontractor, Nick Del Rosso. Court records allege that Del Rosso paid \$1 million to Indian hacking company CyberRoot, which worked with another firm, BellTroX, to break into the emails of RAKIA's former business partner, American-Iranian airline executive Farhad Azima.



Azima is currently suing RAKIA, Dechert and Del Rosso over the intrusion, which he says was carried out so that RAKIA could win a lawsuit against him in Britain. RAKIA recently told a court in London that while it did not "authorise or procure any hacking of Mr. Azima's data" it would not fight his claim. Dechert and Del Rosso are still contesting Azima's suit and deny wrongdoing.

Sources: Court filings in the US and Britain

EXHIBIT 15

Main suspect in potentially momentous hacker-for-hire case seeks plea deal in NY

JULY 2, 2021 BY JOSEPH FITSANAKIS ([HTTPS://INTELNEWS.ORG/AUTHOR/INTELNEWSIOE/](https://intelnews.org/author/intelnewsioe/)) [LEAVE A COMMENT](#)
([HTTPS://INTELNEWS.ORG/2021/07/02/01-3032/#RESPOND](https://intelnews.org/2021/07/02/01-3032/#RESPOND))

IN A DRAMATIC CASE, described by observers as “unusual”, a suspect in a hacker-for-hire scheme of potentially global proportions has told United States government prosecutors he is ready to discuss a plea deal. The case centers on Aviram Azari, a highly sought-after private detective who served in an Israeli police surveillance unit in the 1990s before launching a private career in investigations.

Azari was arrested (<https://www.timesofisrael.com/israeli-held-in-us-for-ties-to-massive-hacking-for-hire-operation/>) in Florida in 2019 during a family vacation, and was shortly afterwards indicted in New York on charges of aggravated identity theft, conspiracy to commit computer hacking, and wire fraud. These charges reportedly date back to 2017 and 2018. Azari’s alleged objective was to target carefully selected individuals in order to steal their personal information, including email usernames and passwords. Last year, *The New York Times* reported (<https://www.nytimes.com/2020/06/09/nyregion/exxon-mobil-hackers-greenpeace.html>) that the case against Azari is connected with a potentially massive hacker-for-hire scheme code-named DARK BASIN.

Further information about DARK BASIN was published (<https://citizenlab.ca/2020/06/dark-basin-uncovering-a-massive-hack-for-hire-operation/>) by Citizen Lab, a research unit of the University of Toronto’s Munk School of Global Affairs and Public Policy, which focuses on information technology, international security and human rights. It said DARK BASIN was orchestrated by an India-based firm called BellTroX InfoTech Services. It also claimed that the company is one of a number of hacker-for-hire firms based in India. These companies are said to be employed by private detectives in Western countries, who are usually hired by large multinationals or wealthy individuals.

Accordingly, the targets of DARK BASIN activities appear to have been investment firms based in the US and elsewhere, as well as government officials, pharmaceutical companies, lawyers, large banks, and even environmental activists who campaign against large multinationals. Additionally, some of DARK BASIN’s thousands of targets appear to be people involved in high-stakes divorce proceedings. Perhaps more alarmingly, among DARK BASIN’s targets are journalists around the world, who seem to have been targeted systematically in efforts to reveal their sources of information.

Azari has pleaded not guilty. But the fact that he his lawyer has now communicated his client’s desire to seek a plea deal with US government prosecutors may be a major game-changer in this case, which may have global ramifications. The Reuters news agency, which reported (<https://www.reuters.com/technology/israeli-charged-global-hacker-for-hire-scheme-wants-plea-deal-court-filing-2021-06-30/>) the latest developments on this case this week, said it reached out to the US Attorney’s Office in Manhattan, but spokesmen there declined to provide any information on Azari’s case.

► Author: Joseph Fitsanakis | Date: 02 July 2021 | Permalink (<https://intelnews.org/2021/07/02/01-3032/>)

FILED UNDER [EXPERT NEWS AND COMMENTARY ON INTELLIGENCE, ESPIONAGE, SPIES AND SPYING](#) TAGGED WITH [AVIRAM AZARI](#), [BELLTROX INFOTECH SERVICES](#), [COMPUTER HACKING](#), [CYBER SECURITY](#), [INDIA](#), [NEWS](#), [OPERATION DARK BASIN](#), [PRIVATE SECURITY FIRMS](#), [UNITED STATES](#)

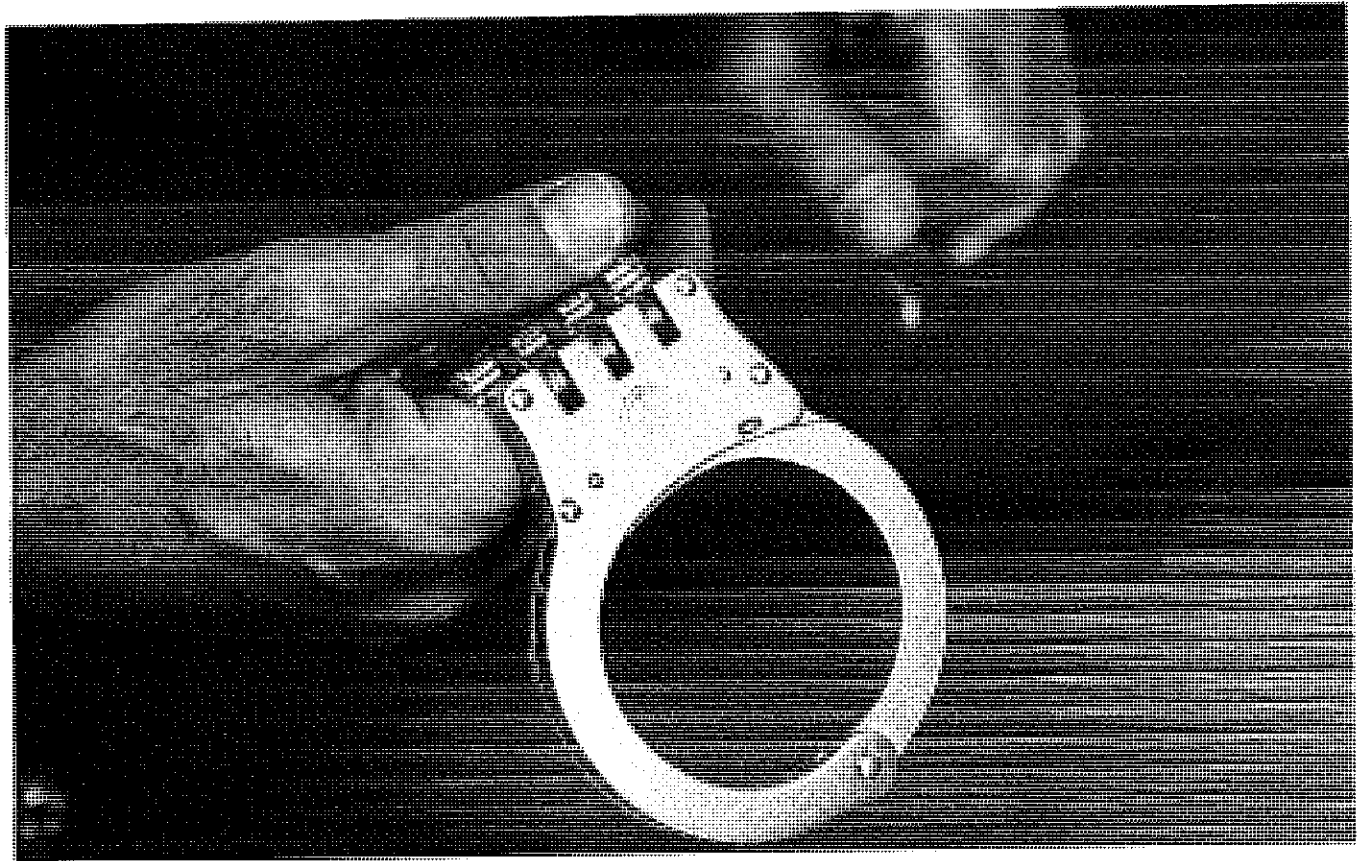
EXHIBIT 16

Israeli held in US for ties to massive hacking-for-hire operation

Private investigator Aviram Azari has been indicted in New York for suspected links to global online criminal campaign, The New York Times reports

By TOI STAFF

10 June 2020, 8:57 pm



Illustrative: A policeman holds handcuffs. (Yossi Zamir/Flash90)

An Israeli arrested last year in the US is a suspect in a wide-ranging federal criminal investigation into a hacking operation against government officials, journalists, environmental activists and others.

Aviram Azari was apprehended in Florida last year during a family trip, and indicted in New York on charges of wire fraud, identity theft and conspiracy to commit computer hacking, The New York Times reported on Tuesday.

Azari appears to be the first suspect taken into custody in the case, which was sparked by phishing emails that targeted environmental groups starting three years ago.



The campaign, dubbed “Dark Basin,” appeared to be part of a sprawling hacking-for-hire operation. The targets, numbering in the thousands, often seemed to take one side of a legal or advocacy issue, or business proceeding.

A primary target was US-based nonprofits. It is unclear how successful the operation has been, and it is likely still active, the report said.

Phishing attacks are a type of fraud where the attackers pose as reliable entities to trick victims into giving up private information, usually for identity theft. Phishing attacks are carried out via email or other online communication.

The Canada-based watchdog group Citizen Lab publicized information on the case on Tuesday. The outfit said the operation was likely handled by a firm in India called BellTroX InfoTech Services, Citizen Lab said.

Azari is accused of using phishing attacks to break into accounts in 2017 and 2018. His alleged accomplices and victims, at least one in New York, were not named.

Azari served in a police surveillance unit and was a coveted private investigator in Israel, The New York Times report said. He has pleaded not guilty.

EXHIBIT 17



PRESS RELEASE

Israeli Hacker-For-Hire Sentenced To 80 Months In Prison For Involvement In Massive Spearphishing Campaign

Thursday, November 16, 2023

For Immediate Release

U.S. Attorney's Office, Southern District of New York

Damian Williams, the United States Attorney for the Southern District of New York, announced that AVIRAM AZARI was sentenced today to 80 months in prison for computer intrusion, wire fraud, and aggravated identity theft in connection with his involvement in a massive computer-hacking campaign targeting companies and individuals in the U.S. and around the world. AZARI was arrested on these charges in September 2019 while traveling to the U. S. from abroad and has been detained since his arrest. U.S. District Judge John G. Koeltl imposed today's sentence.

U.S. Attorney Damian Williams said: "From his home in Israel, Aviram Azari played a major role in orchestrating and facilitating an international hacking-for-hire spearphishing campaign. The conspiracy targeted individuals and companies in the U.S. and abroad, resulting in the theft of data and netting Azari over \$4.8 million in criminal proceeds. Today's sentencing sends an unmistakable message about my Office's firm commitment to prosecuting hackers, domestic and foreign alike."

According to the allegations contained in the Indictment to which AZARI pled guilty, public court filings, and statements made during court proceedings:

From approximately November 2014 to September 2019, AZARI engaged in an extensive spearphishing campaign that targeted individuals and companies in the U. S. and around the globe. AZARI owned and operated an Israeli intelligence firm. Clients hired AZARI to manage "Projects" that were described as intelligence gathering efforts but were, in fact, hacking campaigns specifically targeting certain groups of victims, including climate change activists and individuals and financial firms that had been a critical part of the German payment processing company Wirecard A.G. AZARI paid different hacking groups, including a particular group located in India, to send spearphishing emails to victims of the various Projects. The hacking groups updated AZARI on their progress, including sending him lists that tracked their hacking efforts against specific victims. The hackers also sent AZARI reports, advising when they were successful in accessing victims' accounts and stealing information.

One of AZARI's hacking Projects was focused on targeting individuals and organizations involved with climate change

advocacy. Some of the hacked documents that were stolen from various of the victims' online accounts were leaked to the press, resulting in articles relating to the New York and Massachusetts Attorneys Generals' investigations into Exxon Mobil Corporation's knowledge about climate change and potential misstatements made by Exxon regarding what it knew about the risks of climate change.

Clients of AZARI's Israeli private intelligence company paid AZARI more than approximately \$4.8 million over a nearly five-year period for managing the intelligence gathering and spearphishing campaign. AZARI executed his crimes deliberately and over an extended period primarily for his own self-enrichment. Some of AZARI's thousands of victims have described the devastating personal, financial, and reputational impact AZARI's crimes had on them. Victims have described the persistent and relentless targeting of them and their associates, as well as the theft of their identities and personal data, as "psychological assault" that has caused them "anxiety, paranoia, depression, sleeplessness, and fear," and the victims have expressed continued concerns for their personal safety.

* * *

AZARI, 52, of Kiryat Yam, Israel, pled guilty to one count of conspiracy to commit computer hacking, one count of wire fraud, and one count of aggravated identity theft. In addition to his prison term, AZARI was sentenced to three years of supervised release and was ordered to pay forfeiture of \$4,844,968.

Mr. Williams praised the outstanding investigative efforts of the Federal Bureau of Investigation.

This case is being handled by the Office's Complex Frauds and Cybercrime Unit. Assistant U.S. Attorneys Juliana N. Murray and Olga Zverovich are in charge of the prosecution.

Contact

Nicholas Biase
(212) 637-2600

Updated November 16, 2023

Topic

CYBERCRIME

Component

USAO - New York, Southern

Press Release Number: 23-400

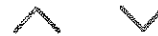
EXHIBIT 18

2:55



< Back

[EXT] Re: Belltrox - Merc...



From: Bing, Christopher (Reuters)
 Sent: Monday, July 11, 2022 2:08 PM
 To: 'Daniel Feldman' <feldman23@gmail.com>
 Cc: Satter, Raphael (Reuters)
 <Raphael.Satter@thomsonreuters.com>
 Subject: RE: [EXT] Re: Belltrox - Mercenary Hacking effort on your account. Story now public.

1/14/16 6:58 Feldman23@gmail.com
failmailurennotice@tech-center.com Mail failure notice

1/19/16 11:11 Feldman23@gmail.com "Twitter"
 <info@twitter.com> We've received report abuse on one of your Twitter Post

1/19/16 11:12 feldmand@yukos.ru "Twitter"
 <info@twitter.com> We've received report abuse on one of your Twitter Post

1/21/16 8:04 sigalfeldman@yahoo.com "=?
 UTF-8?B?RmFjZWJvb2vihKI=?" <noreply-security@facebook.com> We've received a report abuse on one of your posts.

2/15/16 11:31 Feldman23@gmail.com "LinkedIn"
 <noreply-daily-update@linkedin.com> Daniel, confirming your email address will give you full access to LinkedIn

3/16/17 7:24 feldman23@gmail.com "GARY CARR"
 <Garv@delphi.bm> GARY CARR shared "New delphi Management Limited Policies.pdf" with you

3/30/17 6:30 feldman23@gmail.com "Gary Carr"
 <gary@delphi.bm> Please find the attached document of notice.

3/30/17 7:27 feldman23@gmail.com "Google News"
 <news.notification@mail.com> Crude spill hits Venezuela oil port, exports unaffected

3/30/17 9:54 feldman23@gmail.com "Gary Carr"
 <gary@delphi.bm> Confidentials

3/31/17 7:15 Feldman23@gmail.com "David Rourke"
 <David@delphi.bm> Confidentials



EXHIBIT 19

< Back [EXT] Re: Beltrox - Merc... >

From: Satter, Raphael (Reuters)
<Raphael.Satter@thomsonreuters.com>
Sent: Tuesday, July 12, 2022 11:42 AM
To: Daniel Feldman <feldman23@gmail.com>
Cc: Bing, Christopher (Reuters)
<Christopher.Bing@thomsonreuters.com>
Subject: RE: [EXT] Re: Beltrox - Mercenary Hacking effort on your account. Story now public.

UTC timestamp	Target Email	Spoofed Sender	Subject Line
1/13/16 12:45	caleb23@aol.com	"Twitter" noreply-mails@twitter.com	Teri Lindeberg sent you a Direct Message.
1/14/16 5:44	caleb23@aol.com	failmailurennotice@tech-center.com	Mail failure notice
4/9/16 7:13	caleb23@aol.com	info.security@twitter.com	We've received a report abuse on one of your posts.
4/9/16 7:19	caleb23@aol.com	"Twitter" info.security@twitter.com	
3/30/17 7:05	caleb23@aol.com	"Gary Car" gary@delphi.bm	Please find the attached document of notice.
3/30/17 7:22	caleb23@aol.com	"Google News" news.notification@mail.com	Crude spill hits Venezuela oil port, exports unaffected

EXHIBIT 20

Sent: Fri 3/3/2017 7:49:07 AM (UTC)
Subject: New Target Project Yummy
From: [REDACTED]
To: [REDACTED]

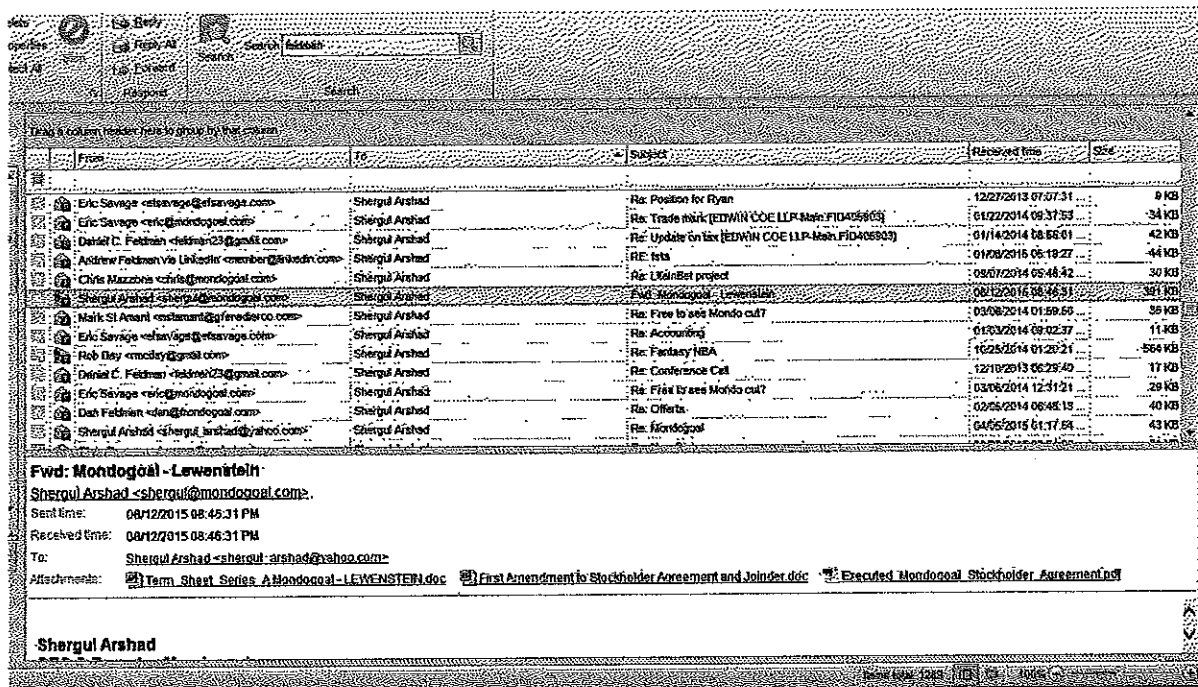
Daniel Caleb Feldman
Feldman23@gmail.com
Caleb23@aol.com
Mobile - +1 646 703 4350

AZ_00061410

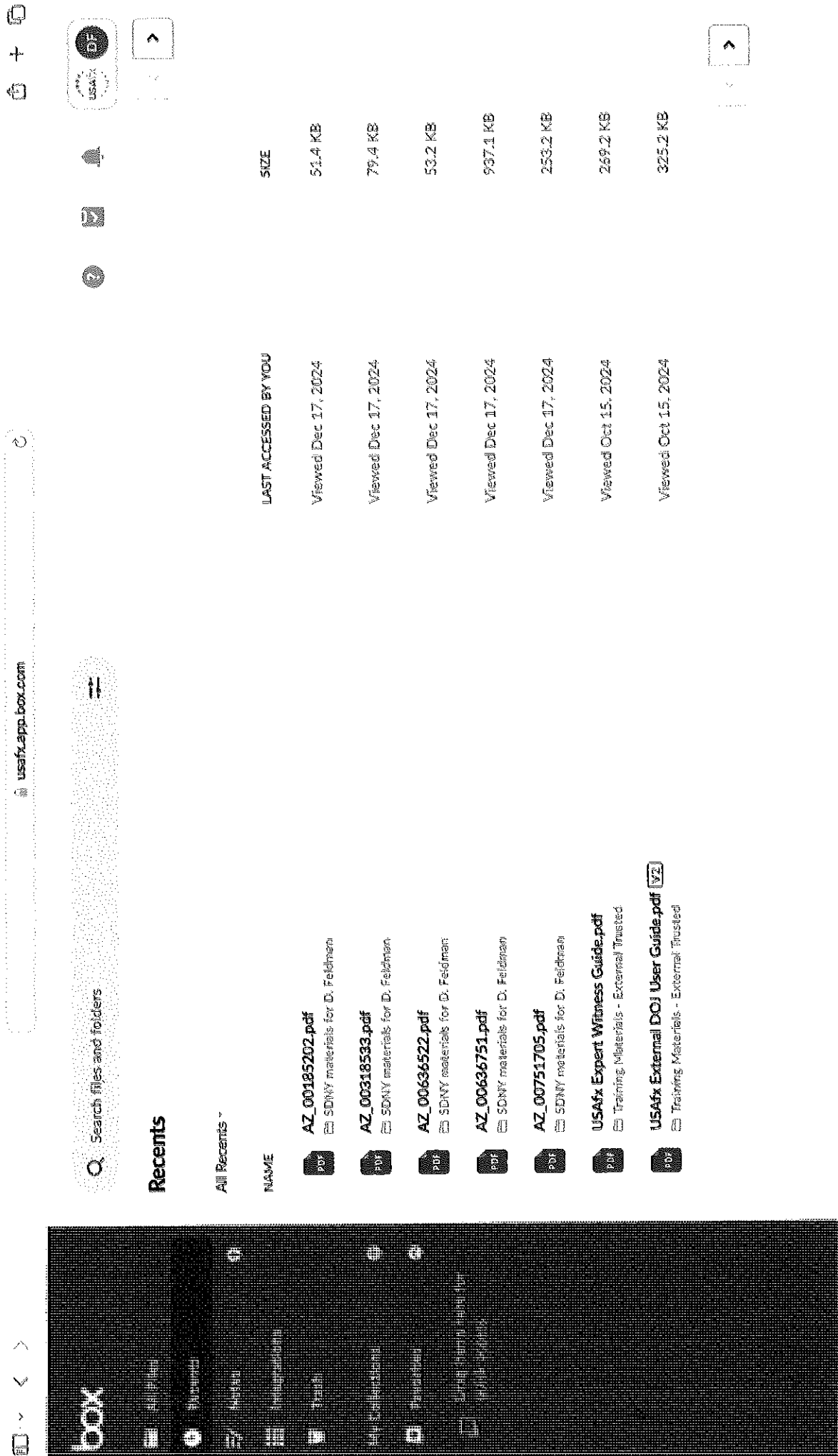
EXHIBIT 21

UTC timestamp (s), Target Email (1&2)	Spoofed Sender (1&2)	Subject Line	Attacker's IP
1/14/16 6:58 Feldman23@gmail.com	failmailurenice@tech-center.com	Mail failure notice	213.152.162.109
1/19/16 11:11 Feldman23@gmail.com	"Twitter" <info@twitter.com>	We've received report abuse on one of your Twitter Post	213.152.162.109
1/19/16 11:12 feldmand@yukos.ru	"Twitter" <info@twitter.com>	We've received report abuse on one of your Twitter Post	104.243.24.236
2/15/16 11:31 Feldman23@gmail.com	"LinkedIn" <noreply-daily-updates@linkedin.com>	Daniel, confirming your email address will give you full access to LinkedIn	94.229.74.91
3/16/17 7:24 feldman23@gmail.com	"GARY CARR" <gar@delphi.bm>	GARY CARR shared "New delphi Management Limited Policies.pdf" with you	82.145.37.203
3/30/17 6:30 feldman23@gmail.com	"Gary Carr" <gary@delphi.bm>	Please find the attached document of notice.	82.145.37.203
3/30/17 7:27 feldman23@gmail.com	"Google News" <news.notification@mail.com>	Crude spill hits Venezuela oil port, exports unaffected	88.150.241.20
3/30/17 9:54 feldman23@gmail.com	"Gary Carr" <gary@delphi.bm>	Confidentials	185.103.96.139
3/31/17 7:15 feldman23@gmail.com	"David Rourke" <David@delphi.bm>	You have been successfully subscribed to Porn.com	
1/15/16 6:03 dan@mondogal.com	noreply.pornhub@lovecat.com	You have been successfully subscribed to Porn.com	
1/15/16 6:14 dan@mondogal.com	adult.service.xsajkubkxna@lovecat.com	We've received report abuse on one of your Twitter Post	213.152.162.109
1/19/16 11:10 dan@mondogal.com	"Twitter" <info@twitter.com>	We've received another report abuse on one of your Twitter Post.	
1/25/16 7:35 dan@mondogal.com	account.teamtwitter@tech-center.com	You haven't reviewed your reported tweets yet	
1/27/16 6:29 dan@mondogal.com	"Twitter" <donoreply@twitter.com>	mNDA- 3 parties Document	213.152.162.79
1/27/16 7:27 dan@mondogal.com	"George N. Gamota, Jr." <ngamotajr.us@verizon.net>	Teresa L. Carlson viewed your profile 9 times on LinkedIn.	173.44.55.155
2/16/16 13:06 dan@mondogal.com	"=PUT-8787GluazV5W7InKl=?=" <no-reply.kr4kw52gmxte@linkedin.com>	Teresa Carlson has shared the following docs:	94.229.74.91
2/16/16 13:07 dan@mondogal.com	"Teresa Carlson (via Google Drive)" <no-reply.alerts.doc@googlemail.com>	We've received a report abuse on one of your posts.	213.152.162.165
3/2/16 6:02 dan@mondogal.com	"Twitter" <notification-hgnsdftrabcc@twitter.com>		

EXHIBIT 22



A2_00318533



EXHIBIT

23

VOORNEMAN GEENEN NOTARISSEN

1

2015VOO18827PRN
Depot akte

DEED OF DEPOSIT

On the eleventh day of September two thousand fifteen appeared before me, -----
Anton Arnaud Voorneman, civil law notary in Amsterdam: -----
Mr Dmitri Grigorievich Merinson, residing at 1072 MK Amsterdam, Marie -----
Heinekenplein 311, born at Moskou, Russian Federation on the tenth day of -----
August nineteen hundred and seventy-three, holder of German passport number --
C7NJPK5F5, married. -----

I recorded that the appearer declared to hand over to me, civil law notary, to keep
in safe custody among my deeds, a private written statement of the appearer dated
the eleventh day of September two thousand fifteen, which private statement shall
be attached to this deed. -----

Thereupon I, the civil law notary, have received the above private statement and -
attached the same to this deed. -----

Furthermore, the appearer requested me to issue true copies of this deed of deposit
and custody with the attached private statement exclusively and only on first -----
written demand of: -----

1. the appearer himself; and/or-----
2. Mrs Ella Yurievna Merinson, residing at 1072 MK Amsterdam, Marie -----
Heinekenplein 311, born at Ekibastuz, former Soviet Union on the thirteenth
day of December nineteen hundred and seventy-five, holder of passport -----
number NP4L9D9F5, married; and/or-----
3. each lawyer practicing at the office of: -----
Bureau Brandeis B.V., -----
with statutory seat in Amsterdam and offices at 1077 AR Amsterdam, -----
Apollolaan 151, filed at the Trade Register of the Chamber of Commerce ----
under number: 58290842. -----

The appearer is known to me, notary.-----

THIS DEED, -----
drawn up, has been executed at Amsterdam, on the day and year mentioned in the
heading in this deed. -----

The contents of this deed were stated and explained in substance to the appearer.
The appearer then declared to be well informed on and to agree with the contents
of this deed and not to care for a reading out in full. -----

Immediately after partial reading, the appearer and I, notary, signed this deed.-----

STATEMENT

For: File civil-law notary (notarial record)
From: Mr Dmitri G. Merinson
Concerning: Written record meeting with Bruce K. Misamore, September 2nd 2015,
16:00 hours CET, Carlton Ambassador Hotel, The Hague
Date: September 11th 2015
Attached: Copy recording conversation and copies valid identifications Mr and
Mrs Merinson

Introductionary statement

I am Dmitri G. Merinson, a Russian and German national born in Moscow on August 10, 1973, employed by Yukos International UK B.V. in the function of Financial Manager/Analyst as of May 20, 2005 (effective April 19, 2005). Before that I was as of February 26, 2003 employed by Yukos Finance B.V. in the function of Managing Director. Since 2002 I worked at the Treasury Department of Yukos Oil Company in Moscow and I opened the Yukos branch office in Amsterdam.

I have a PhD degree in economics and a MBA degree from The University of Chicago. On September 2, 2015 I have met with Bruce K. Misamore at 16:00 hours CET in the Carlton Ambassador Hotel in The Hague. Mr Misamore is (or was, until recently), among other things, director (officer) of Stichting Administratiekantoor Yukos International and Stichting Administratiekantoor Financial Performance Holdings (the "Yukos Foundations") and Yukos International UK B.V. Immediate cause for the aforementioned meeting was an invitation of Mr Misamore.

Written record content conversation

Bruce K. Misamore ("Misamore") informed me that he was compelled to announce in arbitration court in The Hague yesterday that he is no longer a member of the Yukos Foundations' boards and that the termination of this role was not by his own free choice. Misamore told me he gave a speech at the House of Lords of the Parliament of the United Kingdom. I checked on the internet and learned that this must have been on June 18, 2015. Misamore told me Claire Davidson (NB: a former Yukos spokesperson/responsible for PR) was tweeting supposed quotes of Misamore from this speech at the twitter account of The Yukos Library (@TheYukosLibrary)

without his knowledge. Misamore said to me the tweets in question did not represent what he said in his speech, but it caused a legal problem because the co-directors of the Yukos Foundations Godfrey and Fleischman were doing distributions from Stichting Administratiekantoor Financial Performance Holdings. Misamore said that somehow Richard Dietz got knowledge about this distribution and tried to stop it. Misamore told me this was not his fault, that Claire Davidson misquoted him and that he was completely innocent.

Misamore said to me the co-directors (co-officers) of the Yukos Foundations David A. Godfrey ("**Godfrey**"), Steven M. Theede ("**Theede**") and Marc W. Fleischman ("**Fleischman**") nevertheless decided that it was his fault and all board members including Michel de Guillenschmidt ("**Guillenschmidt**") two weeks ago voted against Misamore and removed him from the Yukos Foundations' boards. Misamore told me that now they are forcing him to resign from all the boards of group companies. Misamore said that Godfrey makes it very difficult for him and is aggressive to him. Misamore told me he had to request Tim Osborne ("**Osborne**"), a senior partner of the UK-based law firm Wiggin Osborne Fullerlove, to mediate between him and Godfrey.

Misamore told me there is nothing he could do against this state of affairs and that he had to leave. Misamore said he is trying to sort it out amicably but that he is not happy at all.

I told Misamore about the ambush meeting with Bernard O'Sullivan ("**O'Sullivan**") in London on August 5, 2015 and that I'm ill and under stress. Misamore said to me that Godfrey and his lawyers are doing it now with him and that they are treating him the same way.

I told Misamore what happened about two years ago in Singapore at the bar of the Marina Bay Sands Hotel in the evening where I was together with Steve Wilson during the Mojave meeting trip. There Fleischman came on to us and was very aggressive saying to us that if Feldman and others would not shut up and stop criticizing him we should tell them that he Fleischman would call Brudno and that Brudno would kill them and that Brudno would know how to do that. I and Steve Wilson were shocked by this threat. I told Misamore that later on, somewhere around early 2014 (I don't remember the exact date because I was often in Singapore), I informed Daniel Feldman ("**Feldman**") about this incident because I was concerned for Feldman and his family. I said to Misamore that I advised Feldman to talk with his friend at that time Godfrey about the incident and that he should try not to quote me. I told Misamore that soon after that my difficulties in my relations with Fleischman and Godfrey, who are very close old college friends, started. On February

25, 2014 Fleischman tested me several times in the presence of Martin Parr ("Parr") telling me that Feldman is crazy and that Feldman said to Godfrey that he Fleischman wanted to kill Feldman with Brudno. Later on May 5, 2014 and February 15, 2015 Fleischman demanded my correspondence with Feldman et cetera. I told Misamore that I was afraid, stressed and that I could not respond to them.

I told Misamore about Gretchen King ("King") and that she has interrogated me together with O'Sullivan in London on August 5, 2015 and that Misamore should know how I feel about King. King is responsible for the business intelligence work for Yukos. My impression is that she has a huge budget and I am not aware that there are any controls on her methods.

During the meeting with Misamore on September 2, 2015 I told Misamore again that O'Sullivan (of the international law firm headquartered in London, United Kingdom Olswang LLP, lawyers for Yukos) used my name in a legal opinion dated March 4, 2015 in relation to the "private deal" between YCSarl & YHIL linked with the Rosneft settlement announced on April 1, 2015 without my knowledge and that I found out about this by coincidence only. I told Misamore that this "private deal" was actually done in a secretive way without my and TMF's (TMF Management B.V.) involvement. I told Misamore we found many serious mistakes in the deal documents. Even from the YCSarl side the agreement was signed by Godfrey only (NB: all YCSarl documents require double signatures of both Misamore and Godfrey) and had to sign the documents again after the mistakes were corrected.

Misamore confirmed to me that I am right and that he agrees with me and that they are treating him the same way.

Misamore told me that Godfrey has "mental issues". Misamore said to me Godfrey obtained all the information on Rosneft and Promneftstroy together with King by stealing it from people's laptops and used it in the courts. Misamore told me Godfrey may think that others can do with him the same he did to others. Godfrey doesn't trust anybody, only Fleischman, Misamore said to me.

Misamore told me that I'm most loyal and that he is satisfied with my work. Godfrey and Fleishman don't trust anybody, Misamore said to me. According to Misamore Fleischman is a hitman of Godfrey.

Misamore said he was blasting on Godfrey how he manages business affairs, also he expressed that he was unhappy about how Godfrey and Fleischman are treating me. Misamore said to me he scrutinized Godfrey and Fleischman and that this was also one of the reasons to remove him. Osborne supported Misamore's removal. Theede influenced him, but Misamore is still on good terms with Osborne.

Misamore told me he is still a party in all litigations but that Godfrey wants to control it, for example by not allowing Misamore to use lawyers of his choice like NautaDutilh and deliberately delaying payments to them. Godfrey controls the legal budgets and all trusts.

Misamore told me Godfrey takes care of his buddy Biancamano (NB: an old friend of Godfrey from "Gibson Dunn", a prestigious and selective global law firm headquartered in Los Angeles, United States) and pays their huge invoices without delays and he runs an "open checkbook" for legal expenses.

Misamore said to me Fleischman takes care about his buddies at AllianceBernstein, a global asset management and research firm based in New York, United States providing investment-management and research services worldwide to institutional, high-net-worth and retail investors and that has US\$485 billion in assets under management (NB: AllianceBernstein charges the highest fees compared to all the other banks we have relations with).

Misamore told me that we pay the Bloomberg subscription for Fleischman for his own trading and chatting.

Misamore told me he said all that to Theede, also that Godfrey and Fleischman are hiding information from the rest of the board.

But Misamore told me that Theede and Guillenschmidt support Godfrey and Fleischman. According to Misamore Theede is a wimp. Guillenschmidt is ok, Misamore told me, but Guillenschmidt has never fully recovered from his trauma-accident and is therefore not fully mentally capable.

Misamore said to me he likes everything to be transparent.

Misamore said again to me Godfrey clearly has serious mental issues, such as depression and severe mental problems.

I told Misamore about recent investment review meetings of Fleischman with UBS AG, a Swiss global financial services company that has US\$1,966.9 billion in assets under management, and Swiss-based Falcon Private Bank, and that these meetings mostly take place at Michelin star restaurants of Fleischman's choice. I told Misamore that at the recent restaurant "investment meeting" with the Falcon Private Bank's Chairman, CEO and two female managers of the bank Fleischman came drunk, he told stories how he likes to fly with Godfrey at British Airways first class (not business class), how they are drinking a lot there, how Fleischman used a sleeping pill with alcohol, how he woke up on the floor of the first class cabin, don't remembering anything. After that Fleischman left the dinner while not even opening the bank's investment presentation.

Misamore noted that apart they were paying US\$ 20.000-25.000 for these flights and stayed in the best hotels.

Misamore said to me he never got an answer as to why the board fired him, only just Theede told Misamore that he has a too "high profile", that the rest of the board want to be secretive and that Fleischman wants to have more money. Misamore told me Fleischman was pushing distribution to GMI.

I again raised to Misamore all concerns why Steve Wilson left the board of Mojave and his position of Group Head of Tax, that there are so much "irrational inefficiencies", that Godfrey is in the boards of all companies and that Godfrey solely controls bank accounts without external control, that it's not normal situation when a director controlling accounting records also solely controls all bank accounts and that Godfrey hired a new junior who is not fully qualified for the job tax manager from San Francisco via their common friends at Gibson Dunn.

Misamore started to sign documents which I presented to him for review & approval in his capacity as director of YPBV, YIUKBV & YCSarl, most of legal invoices that were without any breakdowns or back up. Misamore noted that I might need to point out attention of our auditor Marc Lodder to it. Personal legal bills of Godfrey (NB: just to be paid by YIUKBV, I can not see all bills) from Cleber and De Brauw Blackstone Westbroek just for the recent two months exceeded EUR 500.000. Misamore requested to e-mail these fee notes to him.

Misamore said he believes Godfrey should be fired.

Additional statement Mr Merinson

I'm deeply concerned and suspect intentional fraud and the misleading third parties:

1. 2014 accounts of our Luxembourg company Yukos Capital Sarl (a 100% owned sub of Yukos International UK B.V.) are not filed still and not audited – the deadline for filing was July 31, 2015. The intentional delay was caused by Godfrey; Bruce Misamore insisted to file timely, annual accounts were fully prepared by TMF already in the beginning of July!
2. Bruce Misamore was removed from the boards of the Yukos Foundations more than three weeks ago. When I reviewed today on September 11, 2015 the registers of the Dutch Chamber of Commerce this change is still not registered with the Chamber of Commerce. I highly doubt that our auditors in the Netherlands and in Luxembourg are aware of this fact, and of the true reasons for removing Misamore.

Yukos always claimed to be a transparent company, following the highest management and corporate governance standards. At present it's not the case.

Finally, I am in doubt whether I must take further actions/write to the board/write to Theede again (although I know it's useless and will make my position worse and expose me to further harassment – I'm not strong enough to stand up against professional lawyer Godfrey and a bunch of his lawyers enjoying unlimited budget and looting our companies, and the Gretchen King mob). I'm very much afraid and stressed as I've never been in my whole life. It has already affected my health. I can't manage to work with these people, I worked for this company for 14 years and I can not see it going on any longer. I was not able to sleep at all these days. I need help to manage this situation! I like my job but everything what's going on in the recent year is not normal. Sorry for being too emotional. I'm totally exhausted. I want to include this in the notarial statement.

Dmitri G. Merinson

Amsterdam, September 11, 2015

EXHIBIT 24

Martin Parr
Chief Financial Officer
mp@vantageintel.com

Martin has experience in general management, financial management, M&A, restructuring and dispute resolution.

Prior to joining Vantage, he worked for an oil company as part of a small team undertaking divestments, restructuring and high value multi-jurisdiction litigation in order to protect assets and ultimately return funds to shareholders.

Prior to that, Martin worked for many years in progressively more senior roles in UK-based engineering contracting companies operating internationally; in these roles he became experienced in the management of project-based businesses.

Martin is a member of the Chartered Institute of Management Accountants.

Rich Prince

CO-CHIEF FINANCIAL OFFICER

Michael Pochma

VICE CHIEF FINANCIAL OFFICER

X

EXHIBIT 25

J3e2yuk1

1 UNITED STATES DISTRICT COURT
2 SOUTHERN DISTRICT OF NEW YORK

3 YUKOS CAPITAL SARL, et al.,

4 Plaintiffs,

5 v.

15 Civ. 4964 (LAK)

6 DANIEL CALEB FELDMAN,

7 Defendant.

Trial

8 -----x
9 New York, N.Y.
March 14, 2019
10:45 a.m.

11 Before:

12 HON. LEWIS A. KAPLAN,

13 District Judge
-and a Jury-

14 APPEARANCES

15 MORRISON COHEN LLP

Attorneys for Plaintiffs Yukos Capital and Marc Fleischman

16 BY: MARY E. FLYNN

JEFFREY D. BROOKS

17 BARTLIT BECK HERMAN PALENCHAR SCOTT LLP

Attorneys for Plaintiff Marc Fleischman

18 BY: GLEN SUMMERS

19 MANDEL BHANDARI LLP

Attorneys for Defendant

20 BY: ROBERT GLUNT

21 RISHI BHANDARI

J3e2yuk1

Parr - Cross

1 THE WITNESS: I thought I heard your Honor say
2 something.

3 THE COURT: I sneezed. I'm sorry.

4 A. Yes.

5 Q. And what company are you a director of that provides
6 business intelligence services?

7 A. Vantage Intelligence U.K. Ltd.

8 Q. Is that formerly known as One Touch Intelligence?

9 A. I am not aware of that. If it is, I should be aware of it.
10 But, no, I'm not aware of it.

11 Q. Now, that company -- does that company provide services to
12 the Yukos Group?

13 A. No.

14 Q. Does it ever?

15 A. No.

16 Q. Let's talk about Cleanthis Georgiades. He is a former
17 director of Yukos Hydrocarbons, correct?

18 A. Correct.

19 Q. And his firm, GE Law, used to provide services for Yukos
20 Hydrocarbons, correct?

21 MS. FLYNN: Objection, your Honor. Beyond the scope
22 of direct.

23 THE COURT: Sustained.

24 MR. GLUNT: Your Honor, Mr. Parr is identified on our
25 witness list by designation, but we have designated portions of

EXHIBIT

26

1 S. Theede

2 no --

3 MR. GLUNT: You already said no.

4 MS. FLYNN: -- before I objected, so
5 it's okay.

6 Q. So let's -- let's make this clear
7 and take it a piece at a time. Do you know
8 someone named Gretchen King?

9 A. I've never met Gretchen King. I
10 know the name Gretchen King, but I've never met
11 Gretchen King.

12 Q. Do you know if Gretchen King works
13 for the Yukos Group?

14 MS. FLYNN: Object to the form.

15 When you say "work for," do you mean
16 as an outside vendor or employee?

17 Q. Do you know if Gretchen King
18 provides any services of any kind to the Yukos
19 Group?

20 A. I believe she is a service provider.

21 Q. And what services do you believe
22 Gretchen King provides to the Yukos Group?

23 A. I -- I believe she provides certain
24 information in support of litigation that we have
25 ongoing.

1 S. Theede

2 Q. Who, if anyone, hired Gretchen King
3 to provide that information?

4 A. Presumably it would have been Dave
5 Godfrey.

6 Q. When -- is Mr. Godfrey -- well,
7 strike that.

8 Who approved the payment that
9 Gretchen King receives for providing that
10 information, if any?

11 A. I'm assuming Dave Godfrey would have
12 approved the -- the invoice or whomever the
13 board -- from whichever entity she would be paid,
14 if she was paid, it would likely be the board of
15 that entity.

16 Q. Are there any Yukos Group entities
17 on which David Godfrey does not serve on the
18 board of directors?

19 A. I -- I don't think I'm aware of any.
20 There may be, but I -- off the top of my head, I
21 can't think of any.

22 Q. You said that Gretchen King provides
23 certain information in connection with
24 litigation. What kind of information was
25 Gretchen King hired to provide?

1 S. Theede

2 A. You know, I don't know anything
3 about the agreement with Gretchen King, or -- or
4 what her -- you know, what the expectations are
5 of her.

6 Q. Are you aware of a settlement that
7 was entered into between certain Yukos Group
8 entities and Rosneft?

9 A. Yes, I am.

10 Q. And did the foundation's board
11 approve that settlement?

12 A. Yes, we did.

13 Q. Did that settlement involve the
14 resolution of legal cases in which Mr. Feldman
15 was named as a defendant?

16 A. I don't know if -- if Mr. Feldman
17 was named.

18 Q. Do you know if Mr. Feldman was ever
19 instructed to find outside counsel to represent
20 him in connection with settling claims from
21 Rosneft?

22 A. Could you say this -- could you ask
23 that again, please?

24 Q. Absolutely.

25 Do you know if Mr. Feldman was ever

EXHIBIT

27

From: **Dave Godfrey** comradekoba@hotmail.com
Subject: **Fwd: ██████ - male escort**
Date: **Dec 8, 2011 at 10:31:08 AM**
To: **Dan Feldman** feldman23@gmail.com

Begin forwarded message:

From: Gretchen King <gkingnyc@gmail.com>
Date: December 8, 2011 5:20:50 AM HST
To: Dave Godfrey <comradekoba@hotmail.com>
Subject: ██████ - male escort

Here is one of the escort services ██████ contacted during a trip to the UK in 07...

-----Original Message-----

From: Matthew Toma
To: Gretchen King
Sent: Fri Nov 16 14:39:50 2007
Subject: RE: Hodder / Lukoil

Hey Gretchen,

Came across this number in ██████'s records while he was in the UK. It ties everything together, Lukoil, Gazprom, Putin, everybody.

ID# 170676 < TWO4FETISH [Men4RentNow.com](http://www.men4rentnow.com) - gay male escorts, gay ...
<<http://www.men4rentnow.com/escorts/gay.escort.two4fetish.html>>

Cellular:, [+447931505809](tel:+447931505809). PREFERS PHONE CONTACT. Email Him. UK - London.
NY - New York City. S, M, T, W, T, F, S. [7am-11am](#). [11am-3pm](#). [3pm-7pm](#).
[7pm-11pm](#) ...
www.men4rentnow.com/escorts/gay.escort.two4fetish.html - 31k -

Well, maybe not everybody. [REDACTED] called 5 times when he was in London.

Thought you might appreciate.

EXHIBIT

28

vantageintelligence.com/about



Verify it's you

New

CLIENTS

INTELLIGENCE

INFLUENCE

CYBER

NEWS

JOIN

Gretchen King

Co-Founder of Vantage Intelligence

gk@vantageintel.com

Gretchen has nearly twenty years of experience in intelligence and asset recovery. She also has extensive experience in human source development and witness recruitment.

Gretchen began her career in Washington DC with a leading international intelligence firm; during her seven-year tenure with this firm, Gretchen became a Director in the New York office of the firm and helped establish one of the firm's European offices.

Gretchen then joined an oil company to establish and lead an in-house intelligence unit; the primary focus of the unit was to provide intelligence and evidence in support of multiple high-value legal disputes. The unit helped preserve more than USD 1 billion in assets, as evidence gathered by the unit contributed to multiple legal victories.

In 2012, Gretchen co-founded Vantage with the stated aim to focus on disputes, complex commercial issues, asset protection and asset recovery.

EXHIBIT

29

[About Us](#)
[x](#)
[vantageintelligence.com/about](#)
[Error](#)

[Home](#)
[ABOUT US](#)
[CLIENTS](#)
[INTELLIGENCE](#)
[INFLUENCE](#)
[CYBER](#)
[NEWS](#)
[JOBS](#)
[CONTACT](#)

Founders

Gretchen King
CO-FOUNDER OF
VANTAGE INTELLIGENCE

Masha Shvetsova
CO-FOUNDER OF
VANTAGE INTELLIGENCE

Aron Shaviv
FOUNDER OF
VANTAGE INFLUENCE

Executive Management

Eugene Dizenko
MANAGING DIRECTOR

Arseny Barkovskiy
HEAD OF CYBER & FIELD OPERATIONS

Martin Parr
CHIEF FINANCIAL OFFICER

Fay Al-Hakim
CHIEF OPERATING OFFICER

Advisory Board

Erik Prince
US VETERAN AND ENTREPRENEUR

Michael Pochna
INVESTOR AND ENTREPRENEUR

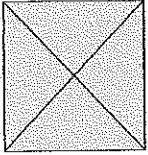
EXHIBIT

30

From: info@twitter.com
To: Feldman23@gmail.com
Subject: We've received report abuse on one of your Twitter Post
Sent: 19-Jan-16 at 11:08:35am GMT

AZ_00081494

Sent: Fri 9/7/2018 11:28:18 AM (UTC)
To: feldman23@gmail.com
From: Helpdesk Team@ <helpdeskeveryday@gmail.com>
Subject: Mail delivery failed!



Mail delivery failed!

There was a problem delivering your email. If you think you are seeing this in error please visit below link and request to resolve the issue.

<https://www.google.com/login/support/report-error/safdbui4bwnojb4d43b5njk>

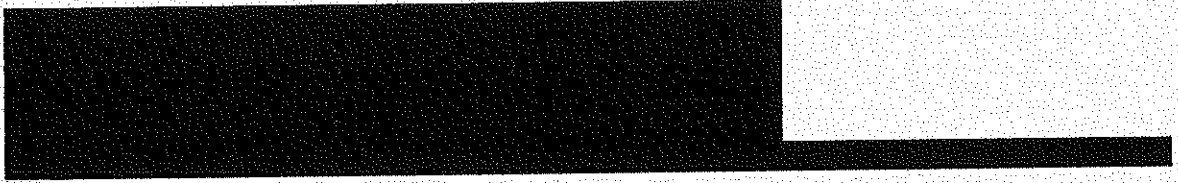
See the technical details below and resolve this issue.

The response was:

554 Message not allowed - [299]
We restricted your outgoing messages because of violation of our policy.

AZ_00327330

Sent: Thur 4/6/2017 12:23:58 PM (UTC)
Subject: Guy gets to spurt his salty seeds in her pussy
From: YouPorn <noreply.535466586you6585tubadh@gmail.com>
To: feldman23@gmail.com

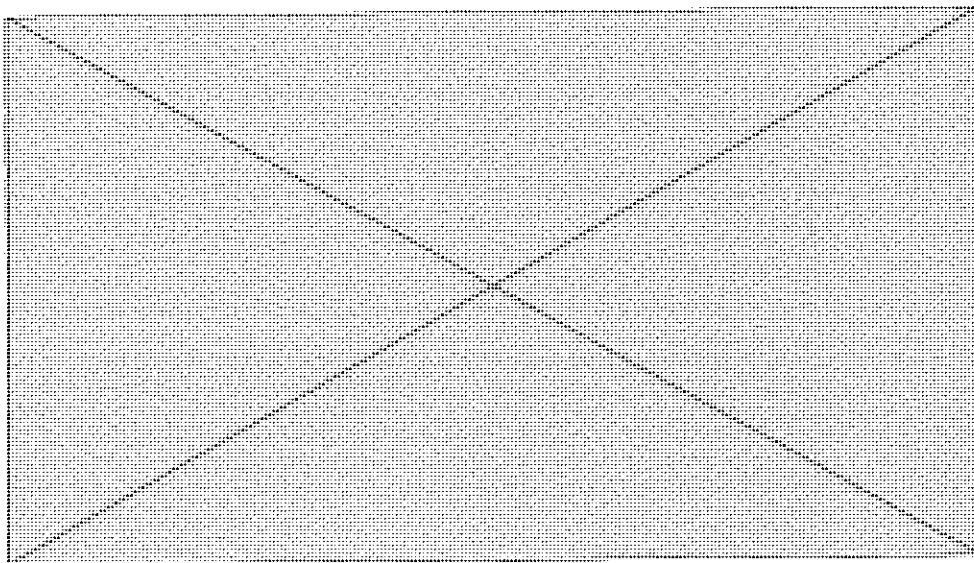


Welcome to our Youporn Service.

Hello,

Your daily love dose YouPorn

If Video/Image is not displayed, Click display Image



AZ_00356266



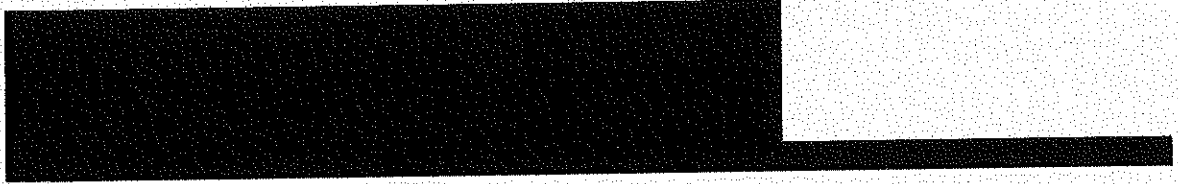
All the best,
Youporn Team.

NOTE: If you received this email in error and did not sign up for a Youporn account you can simply [Unsubscribe](#) this email

This email was sent to feldman23@gmail.com from YouPorn.com
To control which emails you receive from Youporn adjust your email preferences.
[Youporn Blog](#) • [Youporn on Twitter](#) • [Support](#) • [Privacy Policy](#)

AZ_00356266

Sent: Thur 4/6/2017 12:26:48 PM (UTC)
Subject: Sucking and fucking my dildo in just my furry hoodie and Uggs
From: YouPorn <noreply.535466586you6585tubadh@gmail.com>
To: feldman23@gmail.com

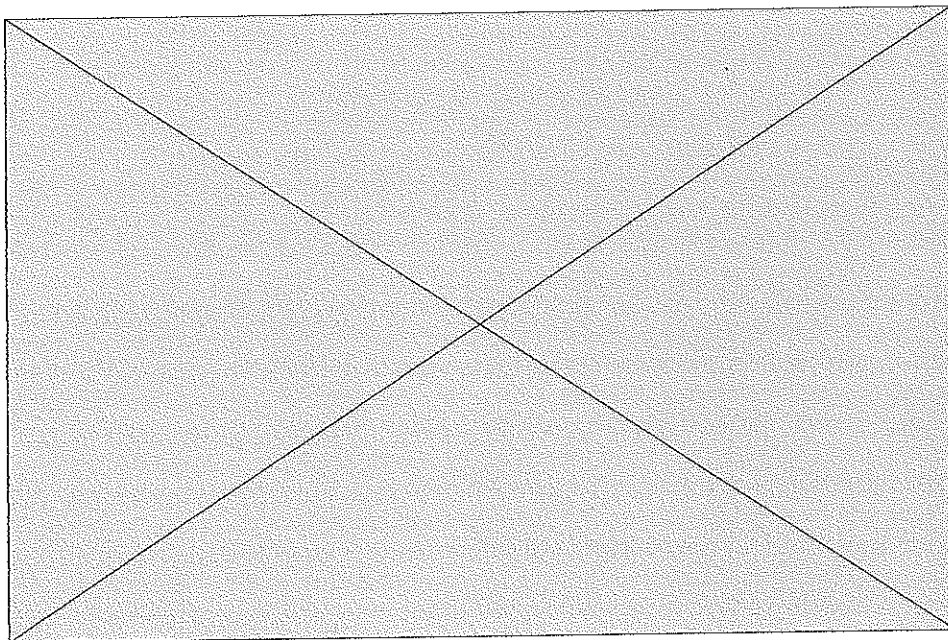


Welcome to our Youporn Service.

Hello,

Your daily love dose YouPorn

If Video/Image is not displayed, Click display Image



AZ-00356272



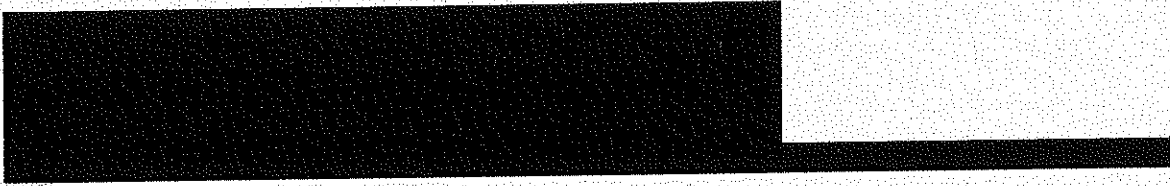
All the best,
Youporn Team.

NOTE: If you received this email in error and did not sign up for a Youporn account you can simply [Unsubscribe](#) this email

This email was sent to feldman23@gmail.com from YouPorn.com
To control which emails you receive from Youporn adjust your email preferences.
[Youporn Blog](#) • [Youporn on Twitter](#) • [Support](#) • [Privacy Policy](#)

AZ_00356272

Sent: Fri 4/7/2017 6:34:03 AM (UTC)
Subject: Stepson Makes Busty Mom Squirt
From: YouPorn <noreply.535466586you6585tubadh@gmail.com>
To: Daniel Feldman <feldman23@gmail.com>

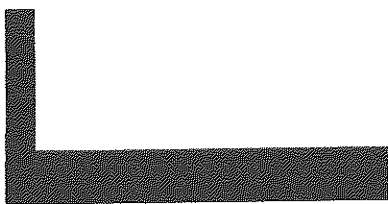
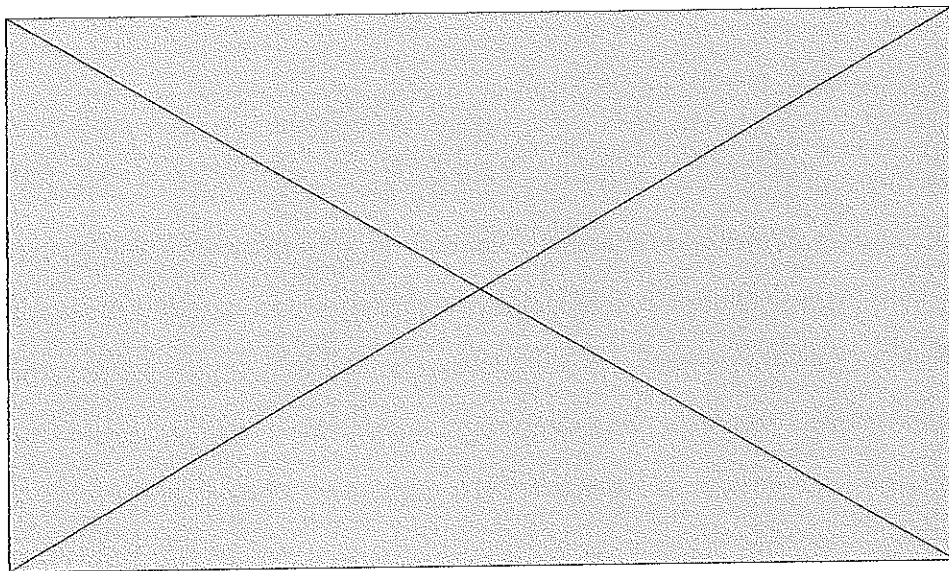


Welcome to our Youporn Service.

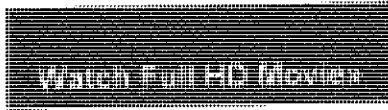
Hello,

Your daily love dose YouPorn

If Video/Image is not displayed, Click display Image



AZ_00356316



All the best,
Youporn Team.

NOTE: If you received this email in error and did not sign up for a Youporn account you can simply [Unsubscribe](#) this email.

This email was sent to jaxmicrane93@gmail.com from YouPorn.com
To control which emails you receive from Youporn adjust your email preferences.
[Youporn Blog](#) • [Youporn on Twitter](#) • [Support](#) • [Privacy Policy](#)

A2_00356316

Sent: Fri 4/7/2017 8:46:55 AM (UTC)
Subject: David Axelrod shared "IMG_1629.JPG" with you
From: David Axelrod <noreply.535466586you6585tubadh@gmail.com>
To: Daniel Feldman <feldman23@gmail.com>

Hi there,

David Axelrod (davidaxelrod@gmail.com) invited you to view the file
"IMG_1629.JPG" on Dropbox.

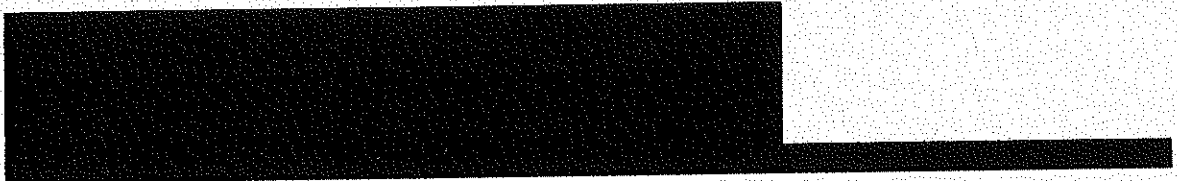
[View file](#)

Enjoy!
The Dropbox team

2017 Dropbox

AZ_00356319

Sent: Fri 4/7/2017 6:41:11 AM (UTC)
Subject: BAEB Best of beautiful brunette babe Leah Gotti
From: YouPorn <noreply.535466586you6585tubadh@gmail.com>
To: Daniel Feldman <feldman23@gmail.com>

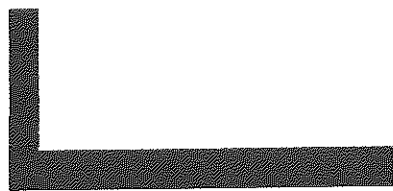
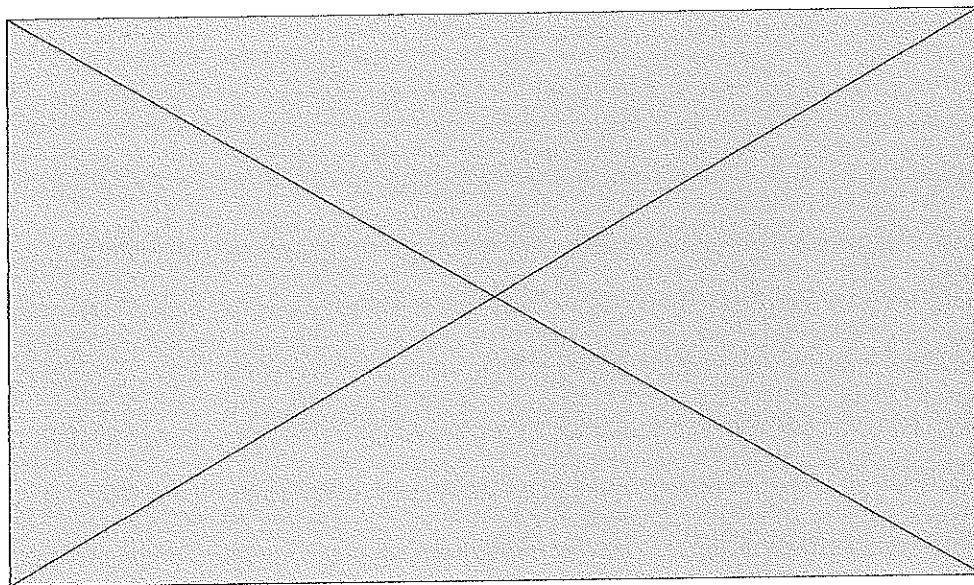


Welcome to our Youporn Service.

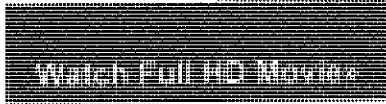
Hello,

Your daily love dose YouPorn

If Video/Image is not displayed, Click display Image



A2_00356327



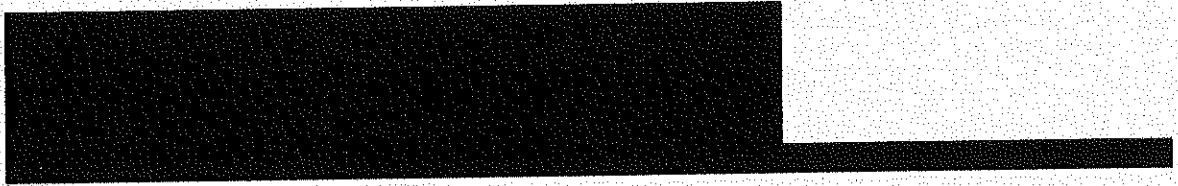
All the best,
Youporn Team.

NOTE: If you received this email in error and did not sign up for a Youporn account you can simply [Unsubscribe](#) this email.

This email was sent to feldman23@gmail.com from YouPorn.com
To control which emails you receive from Youporn adjust your email preferences.
[Youporn Blog](#) • [Youporn on Twitter](#) • [Support](#) • [Privacy Policy](#)

AZ-00356327

Sent: Fri 4/7/2017 6:46:37 AM (UTC)
Subject: Sexy Sheila with her boyfriend
From: YouPorn <noreply.535466586you6585tubadh@gmail.com>
To: Daniel Feldman <feldman23@gmail.com>

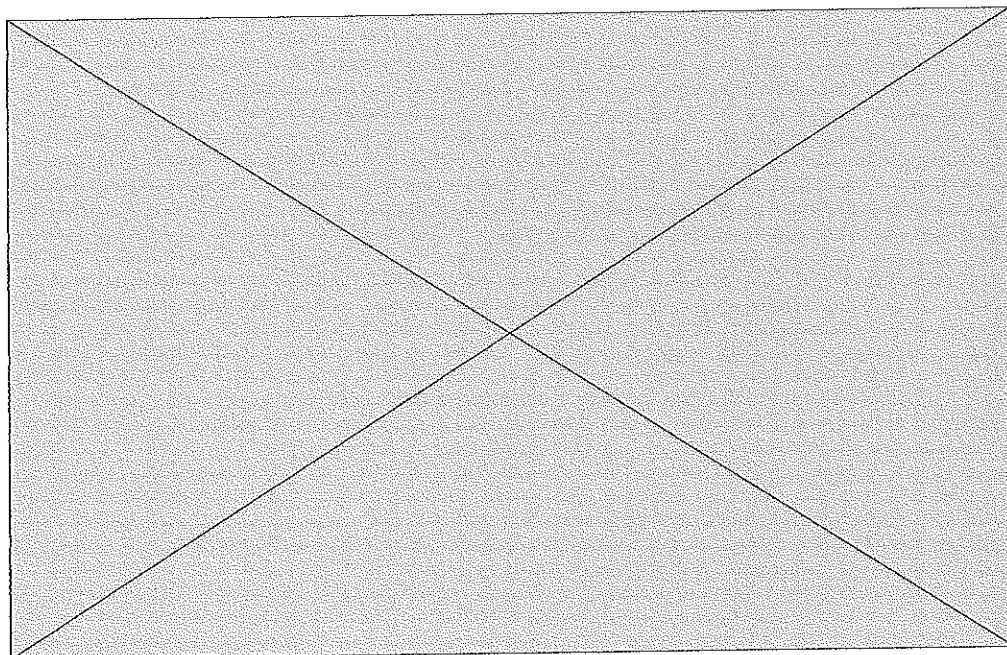


Welcome to our Youporn Service.

Hello,

Your daily love dose YouPorn

If Video/Image is not displayed, Click display Image



AZ_00356330

Watch Full HD Movie»

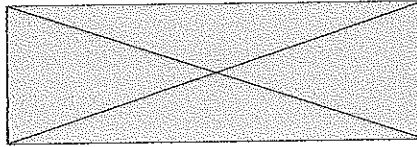
All the best,
Youporn Team.

NOTE: If you received this email in error and did not sign up for a Youporn account you can simply [Unsubscribe](#) this email

This email was sent to feldman23@gmail.com from YouPorn.com
To control which emails you receive from Youporn adjust your email preferences.
[Youporn Blog](#) • [Youporn on Twitter](#) • [Support](#) • [Privacy Policy](#)

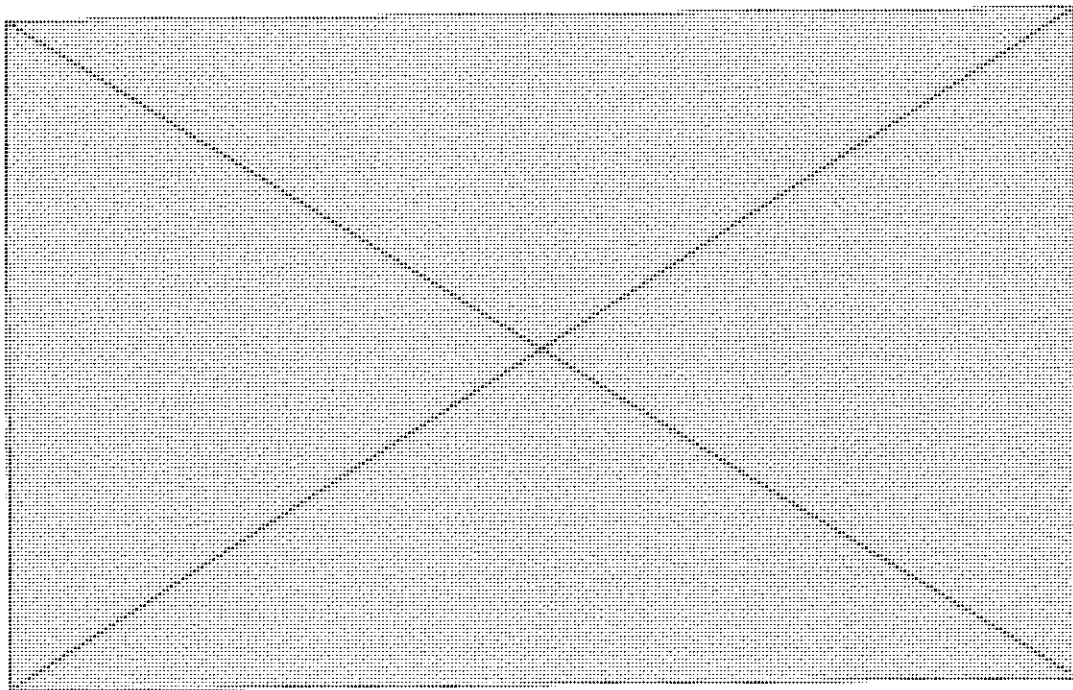
AZ_00356330

Sent: Mon 4/10/2017 5:07:29 AM (UTC)
Subject: NYPD Set to Deploy 1,200 Bodycams Around the City
From: Google News <notification.updatecenter47586@gmail.com>
To: Daniel Feldman <feldman23@gmail.com>



International News

NYPD Set to Deploy 1,200 Bodycams Around the City



By India Today

Published April 10, 2017

The New York Police Department is set to deploy the first body cameras to officers after resolving some of the thorniest issues...(continue reading)

If you don't want to receive newsletter from us then please [Unsubscribe](#).

©2017 Google Inc.

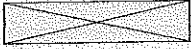


1600 Amphitheatre Parkway, Mountain View, CA 940043

AZ_00356360

Sent: Fri 4/7/2017 12:55:31 PM (UTC)
Subject: do you know Ana Correia, João Ferreira or Eduardo Rosas?
From: LinkedIn <notification.updatecenter57285@gmail.com>
To: Daniel Feldman <feldman23@gmail.com>

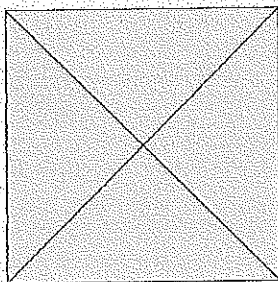
Grow your network to get more out of LinkedIn.



Welcome to LinkedIn

Sachin, LinkedIn is better with connections!

See what your colleagues and classmates have been up to. Add them as connections.

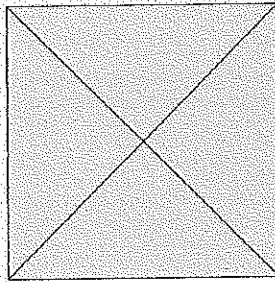


Ana Correia

A procurar novos desafios



Connect

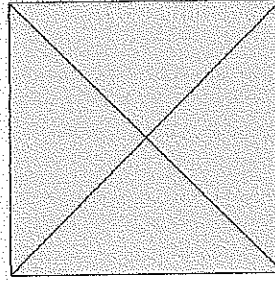


João Ferreira

Produção de ferramentas...



Connect

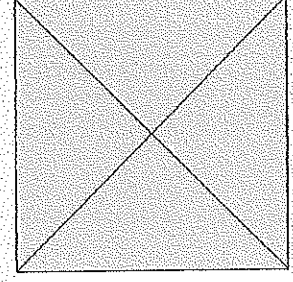


Eduardo Rosas

Photographer | Photojournalist...



Connect



Emanuel Silva

Consultor Imobiliário



Connect

See more people you may know

A2_00356363

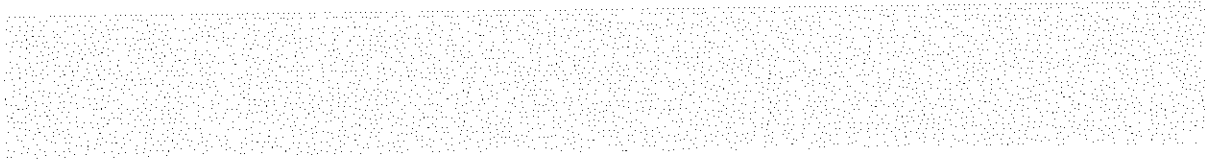
This is an occasional email to help you get the most out of LinkedIn. [Unsubscribe](#)

This email was intended for Louise Lane (Attended Cambridge College). Learn why we included this.
If you need assistance or have questions, please contact LinkedIn Customer Service.

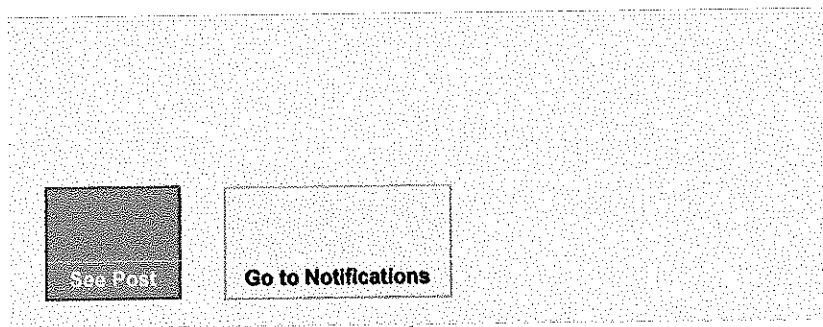
LinkedIn is a registered business name of LinkedIn Ireland Unlimited Company,
Registered in Ireland as a private unlimited company, Company Number 477441
Registered Office: Wilton Plaza, Wilton Place, Dublin 2, Ireland

AZ_00356363

Sent: Fri 5/12/2017 12:19:51 PM (UTC)
Subject: Rebecca Alessandra Giacchi tagged you in a post on Facebook: "Love you sweet heart"
From: Facebook <n0tificati0n.faceb00kmail.jhgjhjhghjgh@serverfortechhelp.com>
To: Daniel Feldman <feldman23@gmail.com>



Rebecca Alessandra Giacchi tagged you in a post on Facebook: "Love you sweet heart"



A2_00357602



If you don't want to receive these emails from Facebook in the future, please [unsubscribe](#).
Facebook, Inc., Attention: Department 415, PO Box 10005, Palo Alto, CA 94303

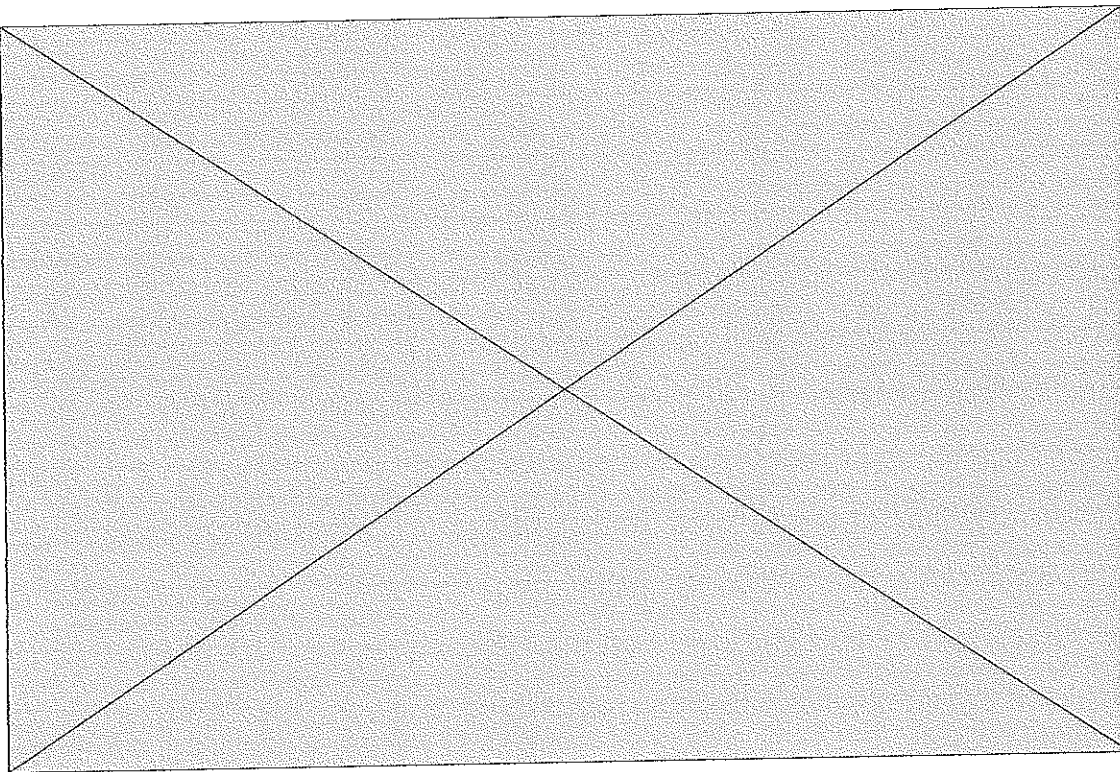
A2-00357602

Sent: Fri 6/9/2017 7:01:42 AM (UTC)
Subject: Pregnant woman stabbed in the neck while riding the subway
From: New York Post <noreply.535466586you6585tubadh@gmail.com>
To: Daniel Feldman <feldman23@gmail.com>

VISIT NYPOST.COM

JUN 09, 2017

Pregnant woman stabbed in the neck while riding the subway



British media are reporting that Conservatives can no longer win an outright majority in Parliament. Sky News reported early Friday that Labour held the seat of Southampton Test, guaranteeing that.....

[Read More](#)

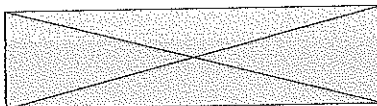
The email address for your subscription is feldman23@gmail.com
[Manage Email Preferences or Unsubscribe](#)

A2-00358809

AZ_00358809

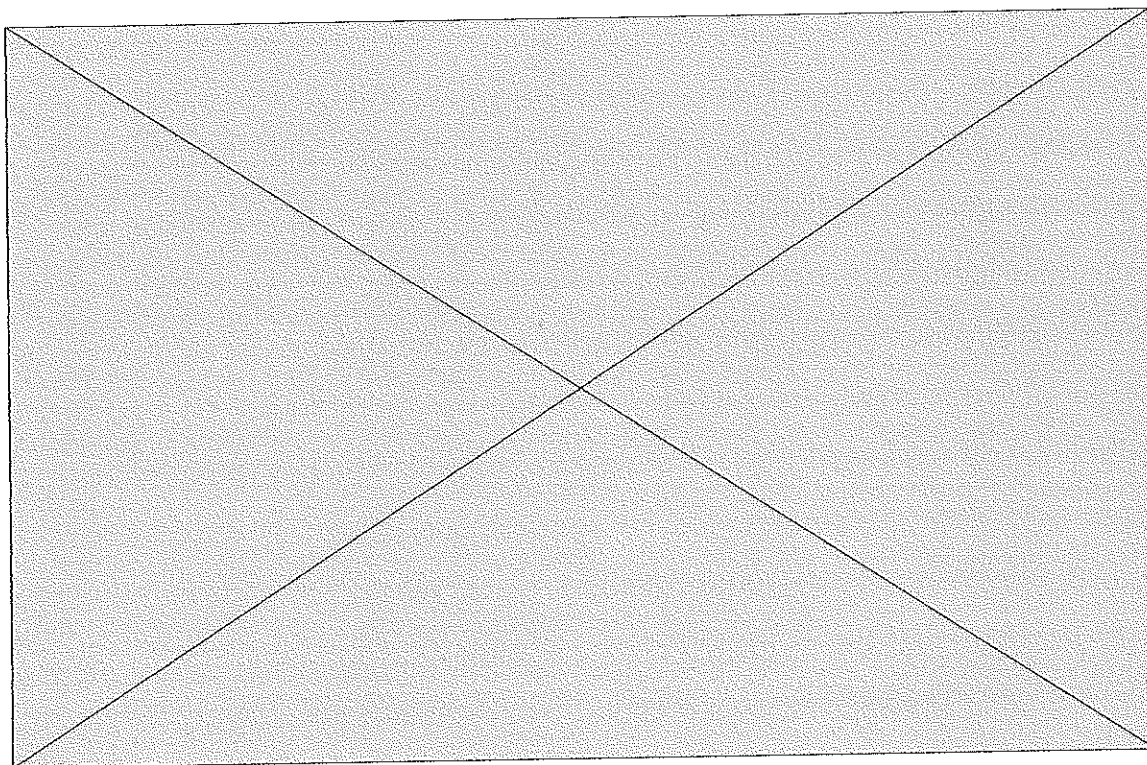
Sent: Fri 6/9/2017 7:11:09 AM (UTC)
Subject: UK election results in hung Parliament in stunning setback for Theresa May
From: New York Post <noreply.535466586you6585tubadh@gmail.com>
To: Daniel Feldman <feldman23@gmail.com>

VISIT NYPOST.COM



JUN 09, 2017

UK election results in hung Parliament in stunning setback for Theresa May



British media are reporting that Conservatives can no longer win an outright majority in Parliament. Sky News reported early Friday that Labour held the seat of Southampton Test, guaranteeing that.....

[Read More](#)

A2_00358820

The email address for your subscription is feldman23@gmail.com
[Manage Email Preferences or Unsubscribe](#)



1211 Avenue of the Americas New York, NY 10036 USA

© Copyright 2017 NYP Holdings, Inc. All rights reserved
[Privacy](#) | [Terms of Use](#) | [Your Ad Choices](#)

AZ_00358820

Sent: Fri 6/9/2017 9:57:18 AM (UTC)
Subject: John O'Kelly-Lynch shared "UFG Private Equity Fund" with you
From: "John O'Kelly-Lynch (via Dropbox)" <noreply.535466586you6585tubadh@gmail.com>
To: Daniel Feldman <feldman23@gmail.com>

Hi Mr. Feldman,

John O'Kelly-Lynch (jokl@delphi.bm) shared "UFG Private Equity Fund" with you on Dropbox.

John said:

"I should have more information for you by close of business tomorrow."

[View on Dropbox](#)

Thanks!

- The Dropbox Team

Want to stop getting invites from Dropbox? [Unsubscribe](#)
Dropbox, Inc., PO Box 77767, San Francisco, CA 94107

© 2017 Dropbox

A2-DD358902

Sent: Mon 6/12/2017 11:44:43 AM (UTC)
Subject: You have been successfully subscribed to Pornhub.com
From: PornHub <noreply.535466586you6585tubadh@gmail.com>
To: Daniel Feldman <feldman23@gmail.com>

Thanks for becoming part of Pornhub service

Your Pornhub account feldman23@gmail.com has been created. Some of your friend has listed your account in our subscription list. Thanks for becoming part of Pornhub service.

Watch now

If you received this email in error and did not sign up for a Pornhub account you can simply [Unsubscribe](#) this email - No further emails will be sent to you.

<https://www.pornhub.com/user/unsubscribe?id=322730711&code=976265952>

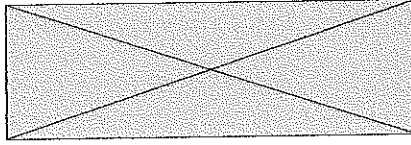
Thanks,
The Pornhub Team

A2_00358985

This email sent from [Pornhub.com](https://www.pornhub.com) to feldman23@gmail.com
To control emails from Pornhub adjust your Email Preferences

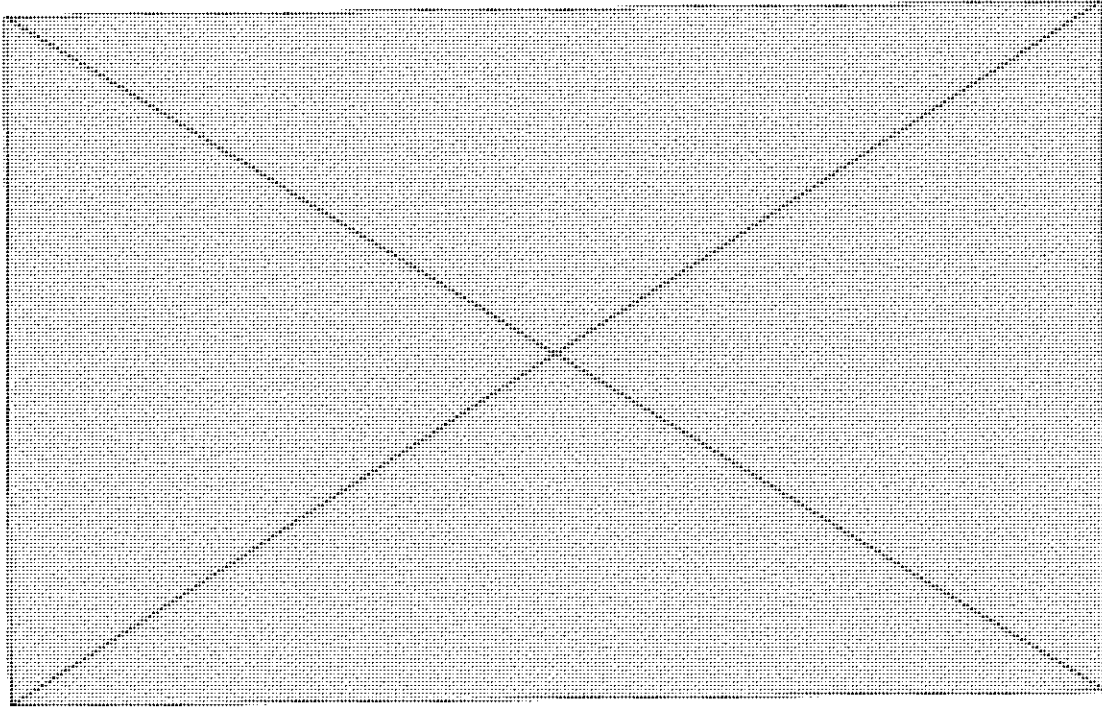
[Pornhub Blog](#) | [Pornhub Twitter](#) | [Privacy Policy](#) | [Contact Support](#)

Sent: Wed 6/7/2017 9:35:04 AM (UTC)
Subject: Fired FBI director Comey 'asked not to be left alone with Trump'
From: Google News <notification.updatecenter47586@gmail.com>
To: Daniel Feldman <feldman23@gmail.com>



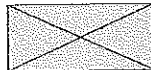
International News

Fired FBI director Comey 'asked not to be left alone with Trump'



By BBC NEWS
Published June 07, 2017

Fired FBI director James Comey told Attorney General Jeff Sessions that he did not want to be left alone with the president...(continue reading)



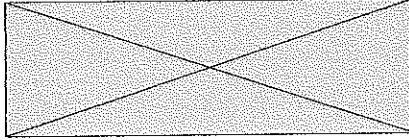
If you don't want to receive newsletter from us then please [Unsubscribe](#).

©2016 Google Inc.

AZ_00359103

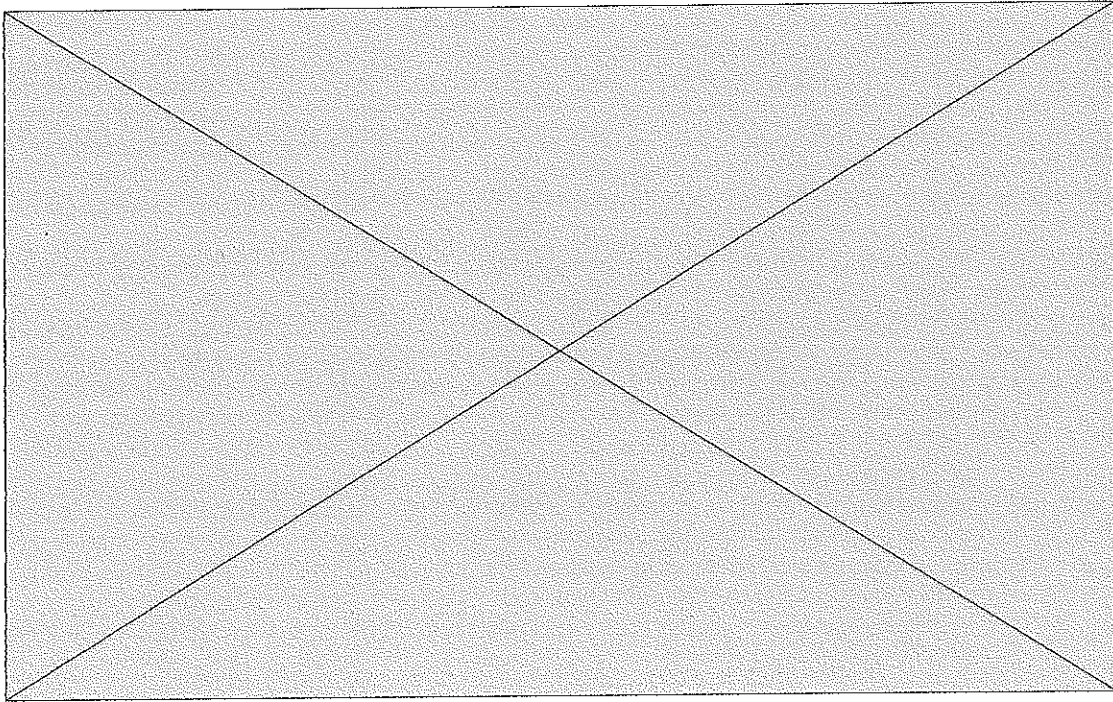
1600 Amphitheatre Parkway, Mountain View, CA 94043

Sent: Wed 6/7/2017 9:44:27 AM (UTC)
Subject: US officials scramble to limit Donald Trump's diplomatic damage over Qatar tweets
From: Google News <notification.updatecenter47586@gmail.com>
To: Daniel Feldman <feldman23@gmail.com>



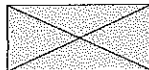
International News

US officials scramble to limit Donald Trump's diplomatic damage over Qatar tweets



By theguardian
Published June 07, 2017

The US state and defence departments have scrambled to limit the diplomatic damage done by Donald Trump's morning...(continue reading)



If you don't want to receive newsletter from us then please [Unsubscribe](#).

©2016 Google Inc.

AZ_00359107

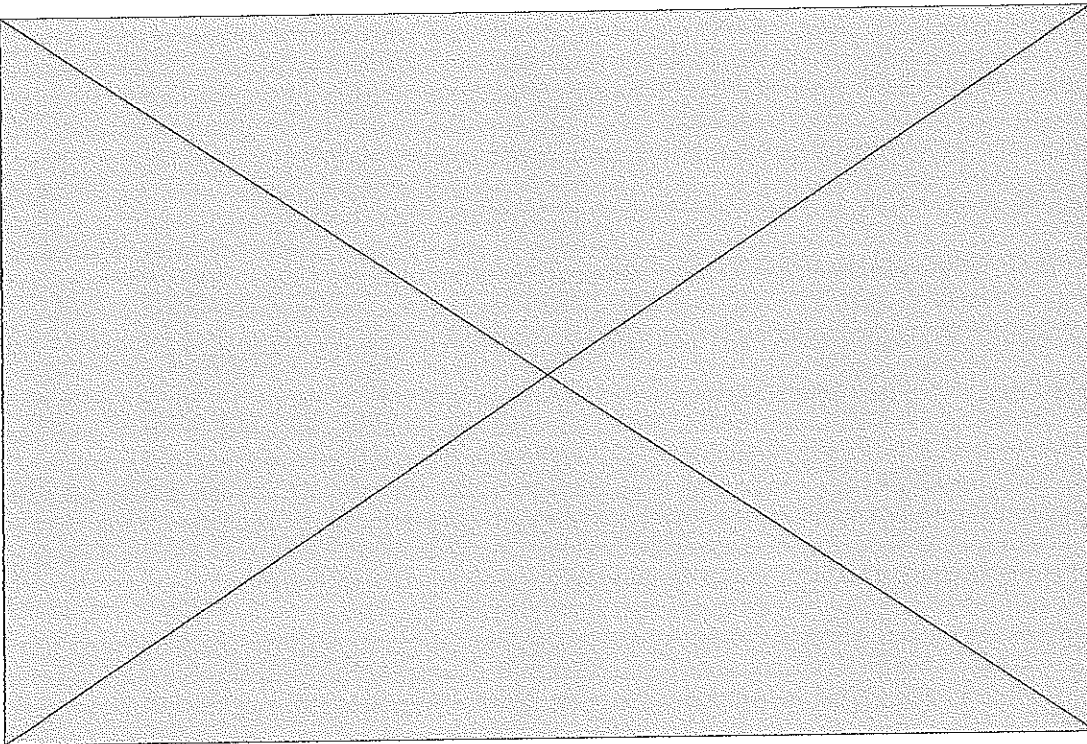
1600 Amphitheatre Parkway, Mountain View, CA 94043

Sent: Tue 6/13/2017 5:45:55 AM (UTC)
Subject: Another federal appeals court rules against Trump's travel ban
From: New York Post <notification.updatecenter57285@gmail.com>
To: Daniel Feldman <feldman23@gmail.com>

VISIT NYPOST.COM

JUN 13, 2017

Another federal appeals court rules against Trump's travel ban



SEATTLE — Another federal appeals court has upheld a decision blocking President Donald Trump's revised travel ban. The ruling Monday from a unanimous three-judge panel of the 9th U.S. Circuit.....

[Read More](#)

The email address for your subscription is feldman23@gmail.com
[Manage Email Preferences or Unsubscribe](#)

New York Post

1211 Avenue of the Americas New York, NY 10036 USA

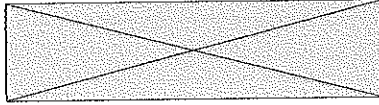
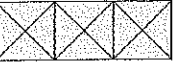
© Copyright 2017 NYP Holdings, Inc. All rights reserved

AZ-00359146

AZ_00359146

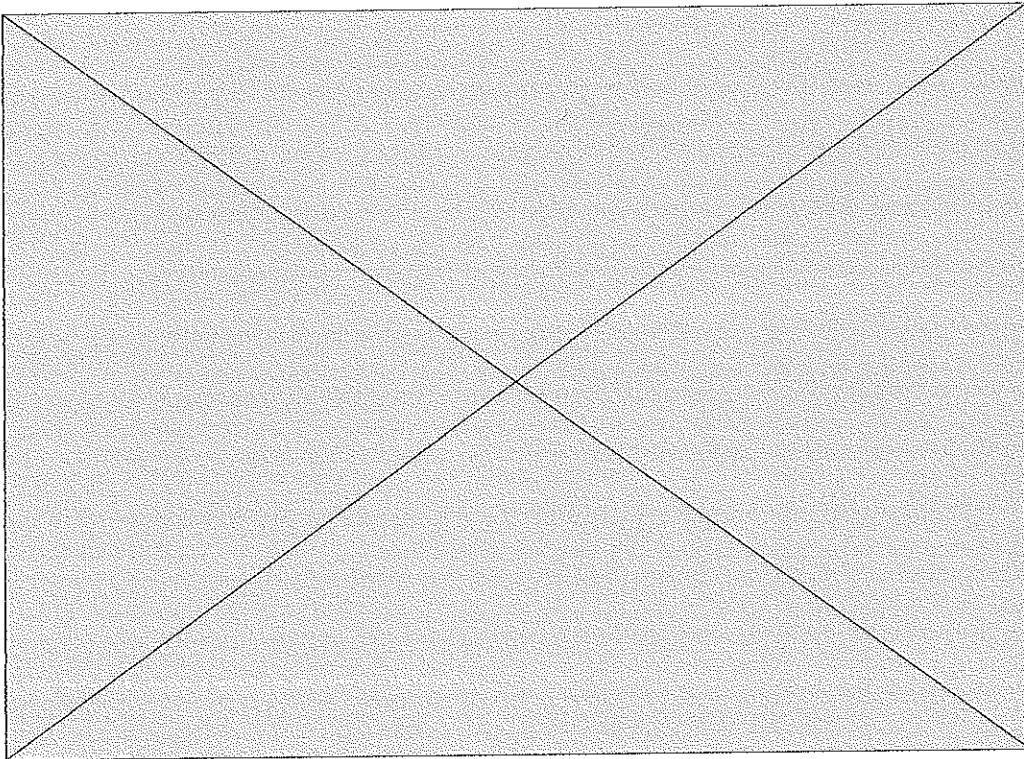
Sent: Wed 6/14/2017 10:36:51 AM (UTC)
Subject: This is exactly how long sex should last
From: New York Post <notification.updatecenter57285@gmail.com>
To: Daniel Feldman <feldman23@gmail.com>

VISIT NYPOST.COM



JUN 14, 2017

This is exactly how long sex should last



Today is National Sex Day – and in celebration of the annual event, it's been revealed how long sex should last.....
[Read More](#)

The email address for your subscription is feldman23@gmail.com
[Manage Email Preferences or Unsubscribe](#)

NYPOST.COM

New York Post
1211 Avenue of the Americas New York, NY 10036 USA

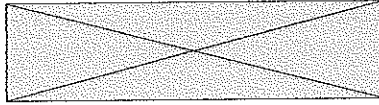
© Copyright 2017 NYP Holdings, Inc. All rights reserved

A2_00359147

A2_00359147

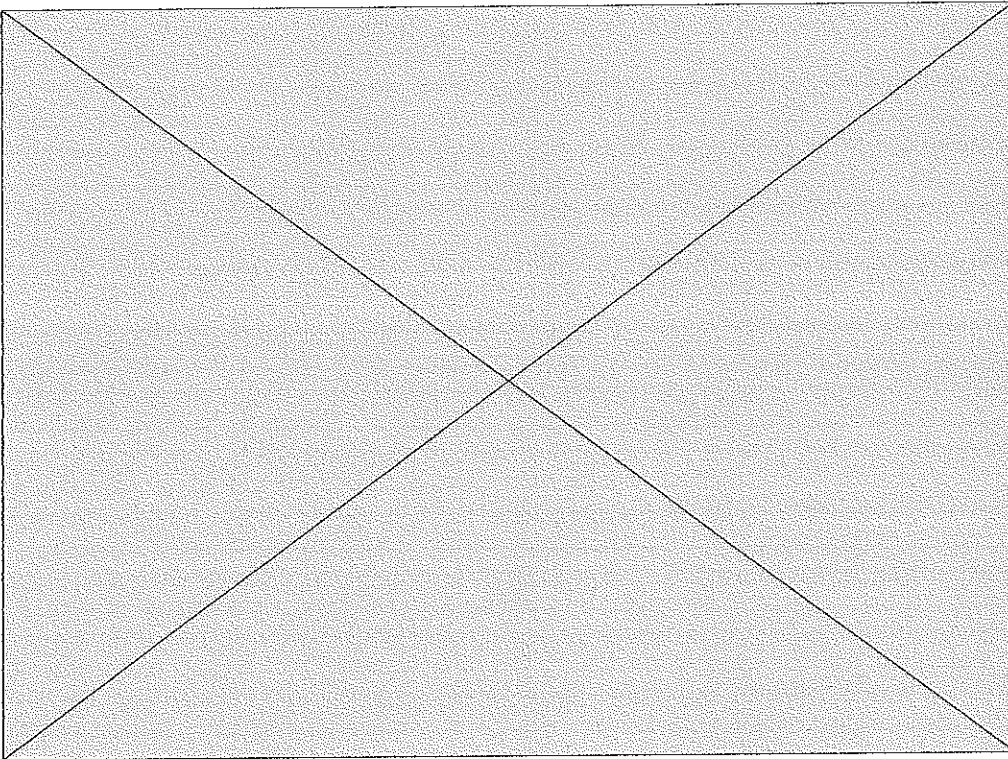
Sent: Wed 6/14/2017 10:46:28 AM (UTC)
Subject: Massive fire breaks out in London high-rise
From: New York Post <notification.updatecenter57285@gmail.com>
To: Daniel Feldman <feldman23@gmail.com>

VISIT NYPOST.COM



JUN 14, 2017

Massive fire breaks out in London high-rise



The London Ambulance service said that 30 patients were taken to five hospitals. They did not give a severity of the injuries, though earlier reports said a number of people were treated for smoke inhalation.....

[Read More](#)

The email address for your subscription is feldman23@gmail.com
[Manage Email Preferences](#) or [Unsubscribe](#)

NYPOST.COM

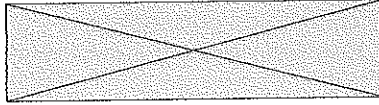
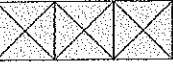
New York Post
1211 Avenue of the Americas New York, NY 10036 USA

AZ-00359156

A2_00359156

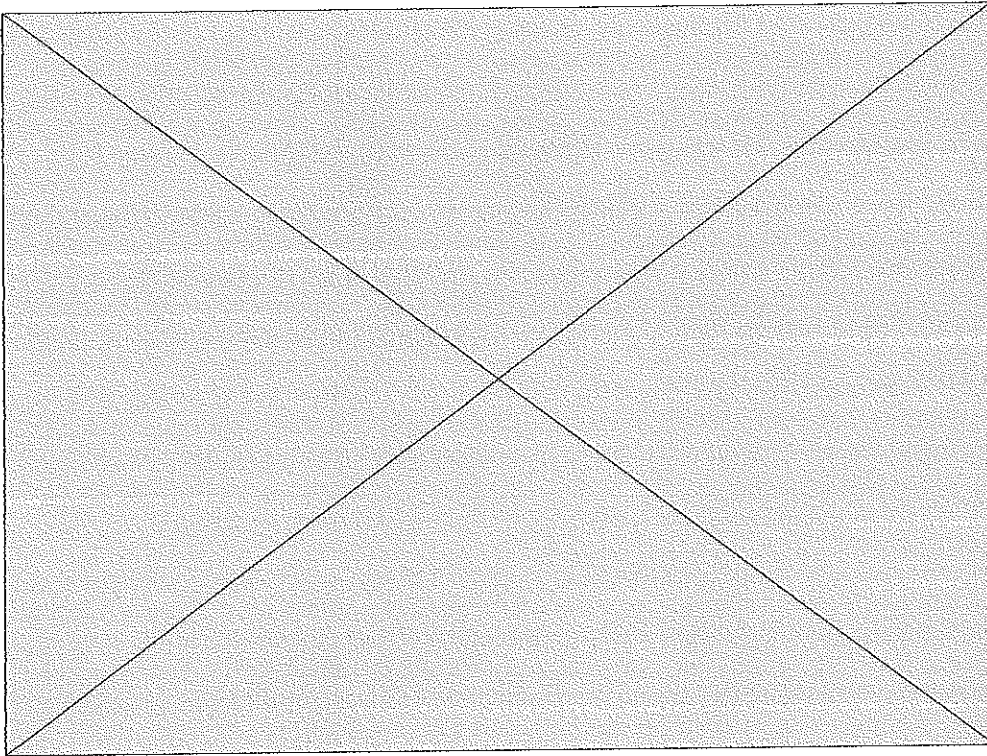
Sent: Wed 6/14/2017 11:08:26 AM (UTC)
Subject: Trump clears way for Pentagon to send more troops into Afghanistan
From: New York Post <notification.updatecenter57285@gmail.com>
To: Daniel Feldman <feldman23@gmail.com>

VISIT NY POST.COM



JUN 14, 2017

Trump clears way for Pentagon to send more troops into Afghanistan



Several U.S. officials say President Donald Trump has given his defense secretary the authority to make decisions on U.S. troop levels in Afghanistan, amid repeated calls from commanders for more forces.....

[Read More](#)

The email address for your subscription is feldman23@gmail.com
[Manage Email Preferences or Unsubscribe](#)

AZ-00359168

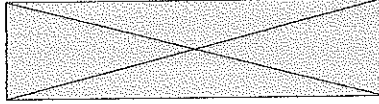
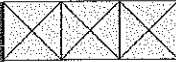
1211 Avenue of the Americas New York, NY 10036 USA

© Copyright 2017 NYP Holdings, Inc. All rights reserved
Privacy | Terms of Use | Your Ad Choices

AZ_00359168

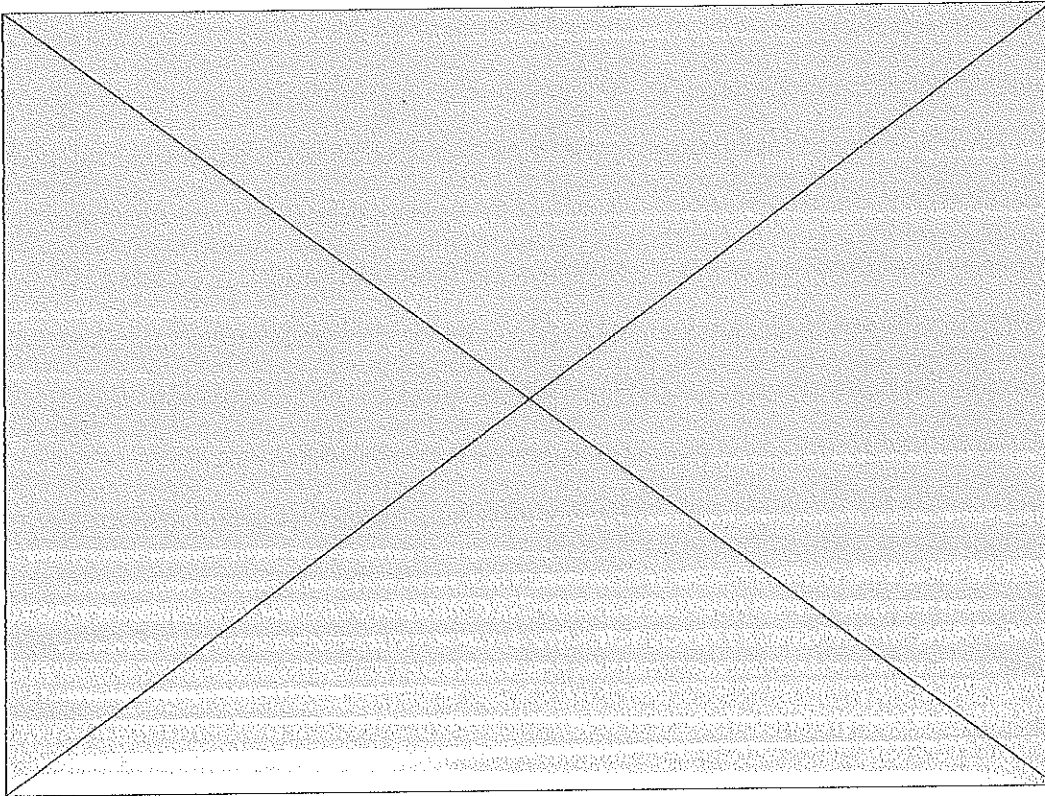
Sent: Wed 6/14/2017 11:49:05 AM (UTC)
Subject: Over 500,000 have applied to join first 'space nation'
From: New York Post <notification.updatecenter57285@gmail.com>
To: Daniel Feldman <feldman23@gmail.com>

VISIT NYPOST.COM



JUN 14, 2017

Over 500,000 have applied to join first 'space nation'



After the creation of Asgardia was announced in Paris last October, more than 500,000 applications were received within the first 20 days, the team behind the project has revealed.....

[Read More](#)

The email address for your subscription is

NYPOST.COM

A2_00359183

© Copyright 2017 NYP Holdings, Inc. All rights reserved
Privacy | Terms of Use | Your Ad Choices

AZ_00359183

Sent: Mon 3/6/2017 7:49:19 AM (UTC)
Subject: You have been successfully subscribed to Youporn.com
From: YouPorn <notification.updatecenter57285@gmail.com>
To: feldman23@gmail.com

Welcome to our Youporn Service.

Hello,

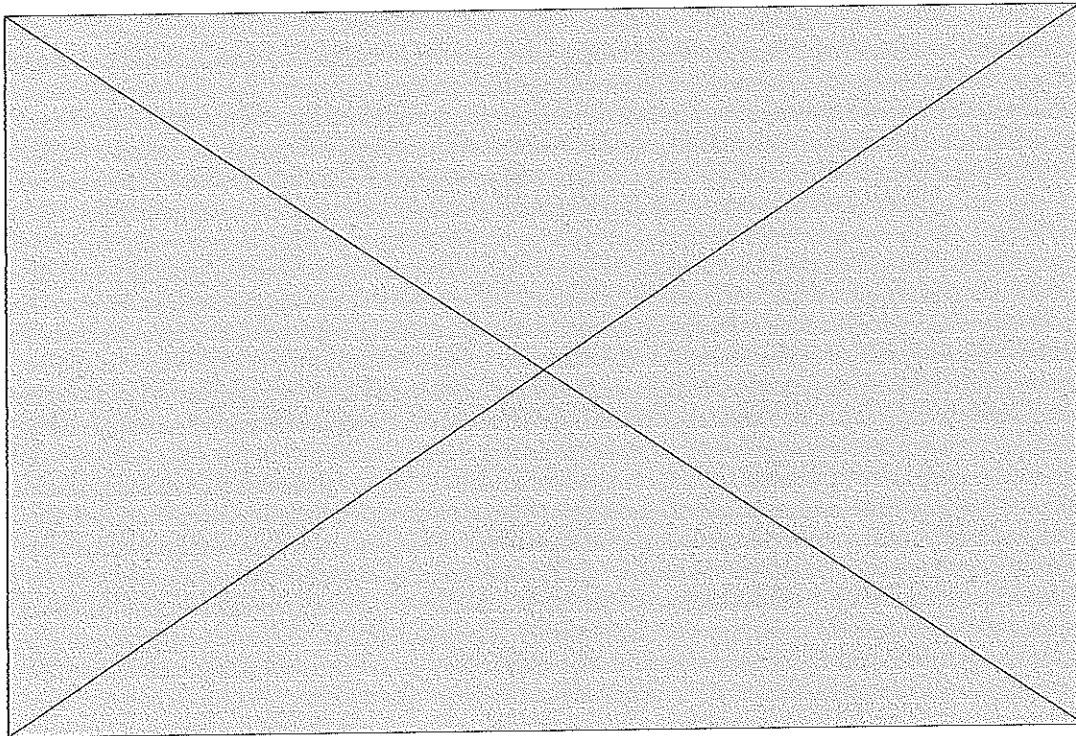
You have been successfully subscribed to YouPorn.com, your account has been activated.

You can go to YouPorn.com to log into your account. Your account information is shown below for reference purposes.

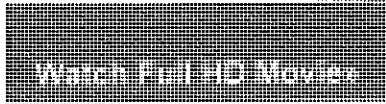
User ID : feldman23@gmail.com

Password : *****

If Video/Image is not displayed, Click display Image



AZ_00634704



All the best,
Youporn Team.

NOTE: If you received this email in error and did not sign up for a Youporn account you can simply [Unsubscribe](#) this email

This email was sent to feldman23@gmail.com from Youporn.com
To control which emails you receive from Youporn adjust your email preferences.
[Youporn Blog](#) • [Youporn on Twitter](#) • [Support](#) • [Privacy Policy](#)

AZ_00634704

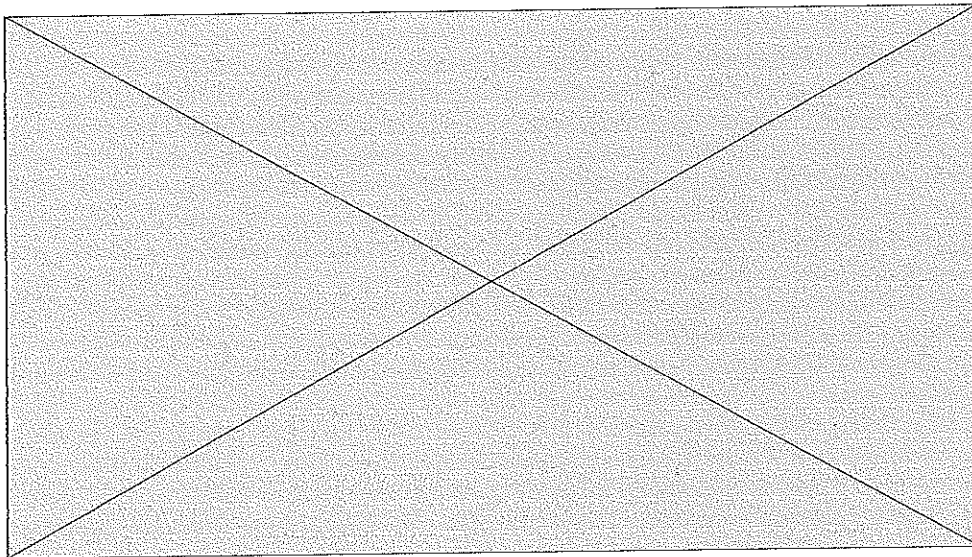
Sent: Mon 3/6/2017 8:43:37 AM (UTC)
Subject: Hot blonde wife gangbanged by plenty of men
From: YouPorn <notification.updatecenter57285@gmail.com>
To: feldman23@gmail.com

Welcome to our Youporn Service.

Hello,

Your daily love dose YouPorn

If the video / image is not displayed, click View Image



[Watch Full HD Movie»](#)

All the best,
Youporn Team.

NOTE: If you received this email in error and did not sign up for a Youporn account you can simply
Unsubscribe this email.

A2_00634711

This email was sent to feldman23@gmail.com from Youporn.com
To control which emails you receive from Youporn adjust your email preferences.
[Youporn Blog](#) • [Youporn on Twitter](#) • [Support](#) • [Privacy Policy](#)

AZ_00634711

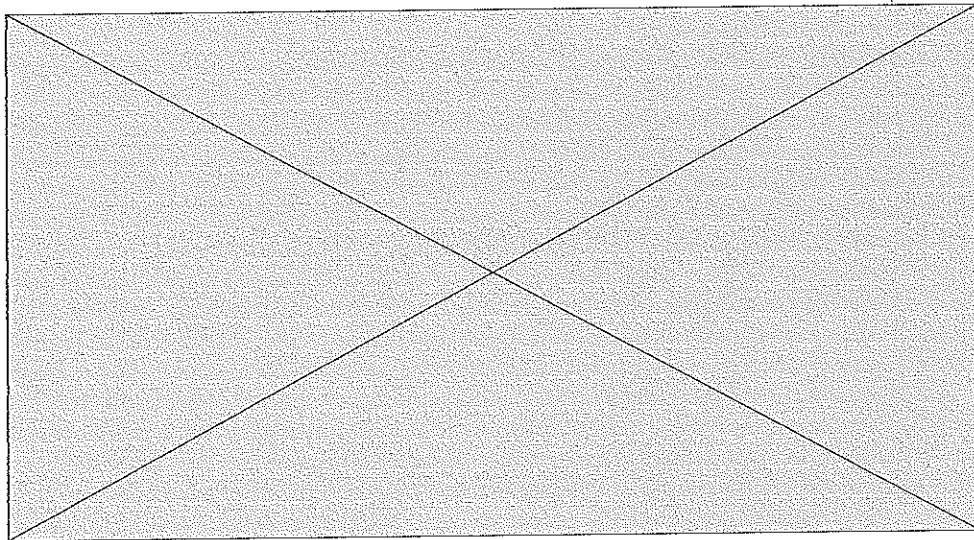
Sent: Mon 3/6/2017 8:44:30 AM (UTC)
Subject: Private Casting X - She loves sucking balls
From: YouPorn <notification.updatecenter57285@gmail.com>
To: Daniel Feldman <feldman23@gmail.com>

Welcome to our Youporn Service.

Hello,

Your daily love dose YouPorn

If the video / image is not displayed, click [View Image](#)



[Watch Full HD Movie»](#)

All the best,
Youporn Team.

NOTE: If you received this email in error and did not sign up for a Youporn account you can simply
[Unsubscribe this email.](#)

A2_00634718

This email was sent to feldman23@gmail.com from Youporn.com

To control which emails you receive from Youporn adjust your email preferences.

[Youporn Blog](#) • [Youporn on Twitter](#) • [Support](#) • [Privacy Policy](#)

AZ-00634718

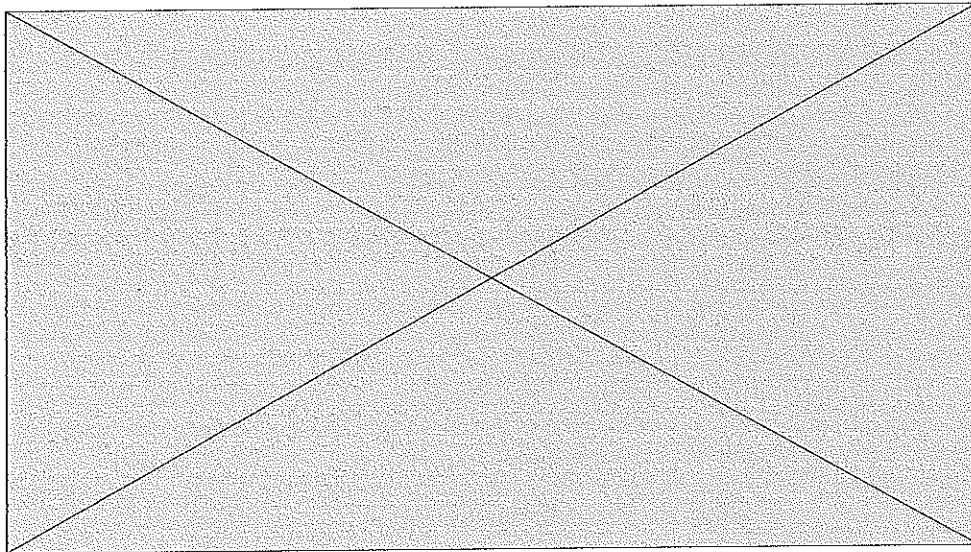
Sent: Mon 3/6/2017 8:45:01 AM (UTC)
Subject: Tina Got Fucked For The First Time WATCH DE
From: YouPorn <notification.updatecenter57285@gmail.com>
To: Daniel Feldman <feldman23@gmail.com>

Welcome to our Youporn Service.

Hello,

Your daily love dose YouPorn

If the video / image is not displayed, click [View Image](#)



[Watch Full HD Movie»](#)

All the best,
Youporn Team.

NOTE: If you received this email in error and did not sign up for a Youporn account you can simply
[Unsubscribe this email.](#)

A2_00634725

This email was sent to feldman23@gmail.com from Youporn.com
To control which emails you receive from Youporn adjust your email preferences.
[Youporn Blog](#) • [Youporn on Twitter](#) • [Support](#) • [Privacy Policy](#)

A2-00634725

Sent: Mon 3/6/2017 8:45:29 AM (UTC)
Subject: Sexy Big Boobs MILF Swallows Young Cock in Sta
From: YouPorn <notification.updatecenter57285@gmail.com>
To: Daniel Feldman <feldman23@gmail.com>

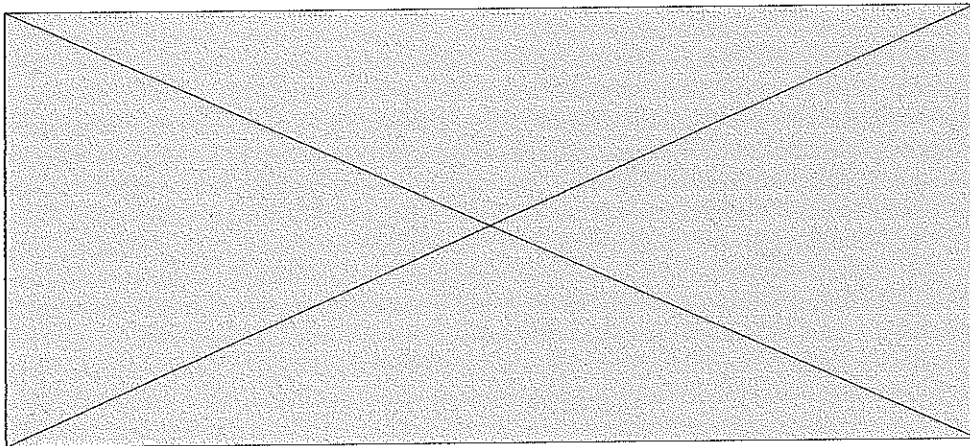
[REDACTED]

Welcome to our Youporn Service.

Hello,

Your daily love dose YouPorn

If the video / image is not displayed, click [View Image](#)



[REDACTED]

[Watch Full HD Movie»](#)

All the best,
Youporn Team.

NOTE: If you received this email in error and did not sign up for a Youporn account you can simply
[Unsubscribe this email.](#)

AZ_00634730

To control which emails you receive from Youporn adjust your email preferences.

[Youporn Blog](#) • [Youporn on Twitter](#) • [Support](#) • [Privacy Policy](#)

AZ-00634730

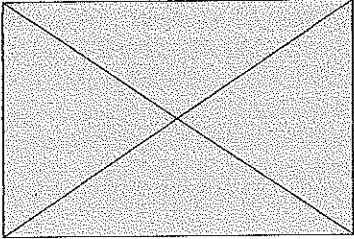
Sent: Mon 3/6/2017 9:13:26 AM (UTC)
Subject: Please keep confidential as I still have to present to Council.
From: David Rourke <noreplynotification.updates@gmail.com>
To: Daniel Feldman <feldman23@gmail.com>

Hello,

Please keep confidential as I still have to present to Council.

Thanks

Drive Link:- https://drive.google.com/32452/new/login.*/final_draft.doc.
Sent from my Samsung Galaxy smartphone.



David Rourke

Delphi Management Limited
Williams House, 4th Floor 20 Reid Street Hamilton, HM 11 Bermuda
Mailing Address: P.O. Box HM 1008 Hamilton, HM DX Bermuda
Telephone: +1 (441) 296-6644
Fax: +1 (441) 296-4283
E-mail: David@delphi.bm

----- Disclaimer -----

This message and any attached files may contain confidential information and are intended only for the person(s) to whom they are addressed. If you are not the intended recipient, please delete this e-mail and attached files from your system and do not use, disclose, copy, print or rely on the e-mail in any manner.

A2 - 00634777

Sent: Mon 3/6/2017 9:18:00 AM (UTC)
Subject: Elsa Antoniou shared Latest Photoshoot with you
From: Elsa Antoniou <elsaantoniou15@gmail.com>
To: Daniel Feldman <feldman23@gmail.com>



Elsa Antoniou shared an album with you

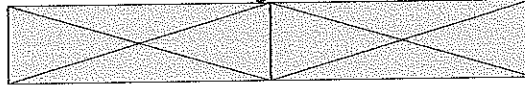
Latest Photoshoot

1

[VIEW ALBUM](#)

You received this mail because Elsa Antoniou shared these photos with you. If you no longer wish to receive email notifications of shared photos, [unsubscribe here](#).

Get the Google Photos app



Google Inc.
1600 Amphitheatre Pkwy
Mountain View, CA 94043 USA

AZ-00634790

Sent: Mon 3/6/2017 9:41:59 AM (UTC)
Subject: Please see the attached document for a copy of cover letter of Delphi Management Limited.
From: Gary Carr <notification.updatecenter57285@gmail.com>
To: Daniel Feldman <feldman23@gmail.com>

Dear,

Please see the attached document for a copy of cover letter of Delphi Management Limited.

https://drive.google.com/13546/new_Delphi-Management-Limited.pdf

Regards,

Gary Carr

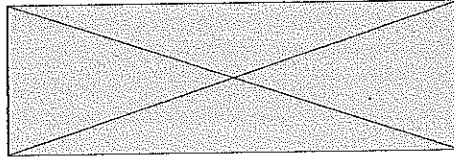
Delphi Management Limited
Williams House, 4th Floor 20 Reid Street Hamilton, HM 11 Bermuda
Mailing Address: P.O. Box HM 1008 Hamilton, HM DX Bermuda
Telephone: +1 (441) 296-6644
Fax: +1 (441) 296-4283
E-mail: Gary@delphi.bm

----- Disclaimer -----

This message and any attached files may contain confidential information and are intended only for the person(s) to whom they are addressed. If you are not the intended recipient, please delete this e-mail and attached files from your system and do not use, disclose, copy, print or rely on the e-mail in any manner.

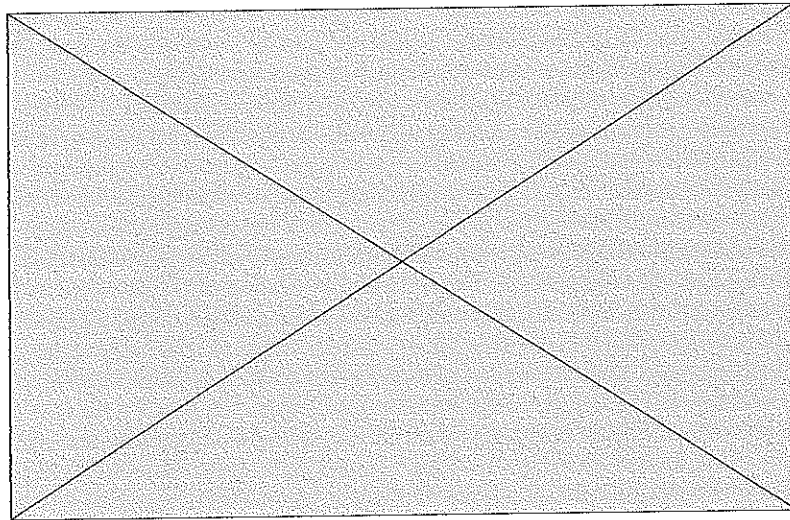
A2_00634821

Sent: Thur 3/23/2017 5:03:59 AM (UTC)
Subject: London attack: Twenty Four dead in Westminster terror attack
From: Google News <notification.updatecenter47586@gmail.com>
To: Daniel Feldman <Feldman23@gmail.com>



International News

London attack: Twenty Four dead in Westminster terror attack



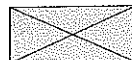
By Google News

Published 05 mins ago

Twenty Four people have died and at least 40 were injured after an attacker drove a car along a pavement in Westminster, stabbed a policeman and was shot dead by police in the grounds of Parliament. (continue reading)

If you don't want to receive newsletter from us then please [Unsubscribe](#).

©2017 Google Inc.



1600 Amphitheatre Parkway, Mountain View, CA 940043

A2-00634905

Sent: Mon 4/17/2017 10:04:13 AM (UTC)
Subject: Your account will be deactivated within 24 hours.
From: Facebook Assistance Team <noreplynotification.updates@gmail.com>
To: Daniel Feldman <feldman23@gmail.com>



Facebook

We've received many report abuse on one of your posts. Your account will be deactivated within 24 hours.

Our Facebook users reported against you for pretending to be someone they're not. We're following up with you about this to make sure you know about the Facebook Community Standards.

We want to keep Facebook safe and welcoming for everyone. Please visit the support dashboard immediately and take a look on the post that got reported.

Alternately you can [click here](#) to confirm your identity via your e-mail ID.

Please co-operate with us immediately, else we may have to take actions according to Facebook Community Standards.



AZ_00635563

Sent: Tue 3/7/2017 6:15:14 AM (UTC)
Subject: Fielding Shawne is waiting for you to see her post on your timeline "Got a little sun today"
From: Fielding Shawne on Facebook <notification.updatecenter57285@gmail.com>
To: Daniel Feldman <feldman23@gmail.com>



Facebook

Fielding Shawne posted on your timeline.



Fielding Shawne

March 07 at 10:34am

Got a little sun today

Got a little sun today



Like



Comment



Edit Email Settings

Reply to this email to comment on this post.

This message was sent from Facebook. If you don't want to receive these emails from Facebook in the future, please **unsubscribe**.
Facebook, Inc., Attention: Community Support, 1 Hacker Way, Menlo Park, CA 940025

A2-00635745

Sent: Thur 3/30/2017 9:19:28 AM (UTC)
Subject: Security alert for your linked Google account
From: "accounts-support-ara@google.com" <notification.updatecenter47586@gmail.com>
To: Daniel Feldman <feldman23@gmail.com>

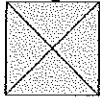


New sign-in from Firefox on Linux

You received this message because feldman23@gmail.com is listed as the recovery email for c****23@aol.com. If c****23@aol.com is not your Google Account, [click here](#) to disconnect from that account and stop receiving emails.

Hi William,

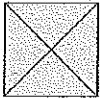
Your Google Account c****23@aol.com was just used to sign in from Firefox on Linux.



Daniel Caleb Feldman

c****23@aol.com

1



Linux

Wednesday, Thursday 30, 2017 2:10 PM (Greenwich Mean Time)

United Kingdom*

Firefox

Don't recognize this activity?

[Review your recently used devices now.](#)

Why are we sending this? We take security very seriously and we want to keep you in the loop on important actions in your account.

We were unable to determine whether you have used this browser or device with your account before. This can happen when you sign in for the first time on a new computer, phone or browser, when you use your browser's incognito or private browsing mode or clear your cookies, or when somebody else is accessing your account.

Best,

The Google Accounts team

*The location is approximate and determined by the IP address it was coming from.

This email can't receive replies. To give us feedback on this alert, [click here](#).

For more information, visit the [Google Accounts Help Center](#).

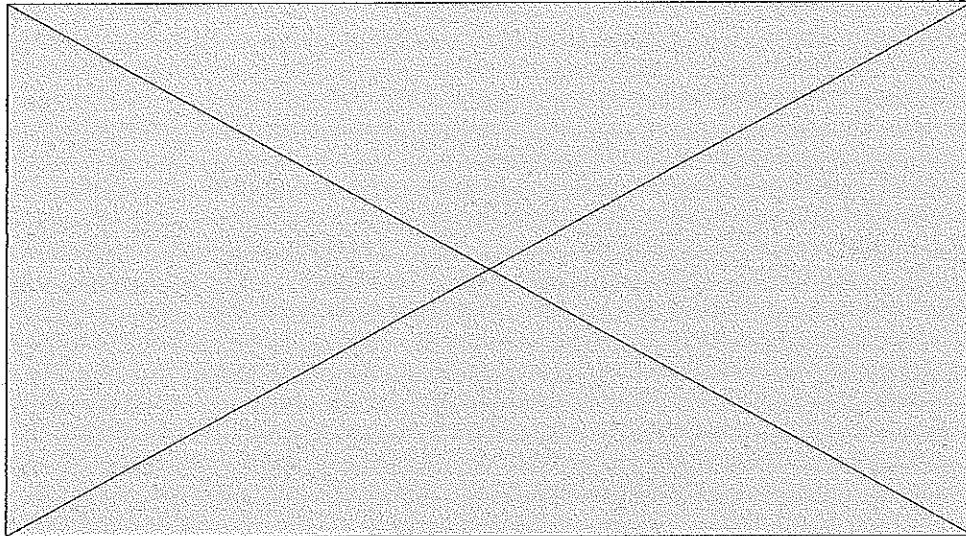
You received this mandatory email service announcement to update you about important changes to your Google product or account.

© 2016 Google Inc., 1600 Amphitheatre Parkway, Mountain View, CA 940043, USA

AZ_00635756

Sent: Thur 3/30/2017 9:41:43 AM (UTC)
Subject: "Interview with Chris Reider and other senior officials of Delphi"
From: YouTube <noreplynotification.updates@gmail.com>
To: Daniel Feldman <feldman23@gmail.com>

Interview with Chris Reider and other senior officials of Delphi



Interview with Chris Reider and other senior officials of Delphi

by Motown India Corporate

Exhaustive Interview with Chris Reider, Vice President, Global Engineering Packard, Electric / Electronic Architecture, Delphi Packard (Shanghai), International Management Company Ltd. Watch Full Video

[Help center](#) • [Report spam](#)

©2017 YouTube, LLC 901 Cherry Ave, San Bruno, CA 94066, USA

AZ_00635773

Sent: Thur 3/30/2017 11:02:50 AM (UTC)
Subject: ♦ UNSUBSCRIBE Now if you want >> feldman23@gmail.com << ♦
From: YouPorn™ <noreplynotification.updates@gmail.com>
To: Daniel Feldman <feldman23@gmail.com>

we are having issue with our
subscribers

If you'd prefer not to receive future emails

we need you to confirm your email by clicking >> here <<

Email Address: feldman23@gmail.com

First Name: Daniel

Last Name: Feldman

If at any time you wish to stop receiving our emails, you can:

> Unsubscribe From Mailing List <

You may also contact us at:

help@youporn.com

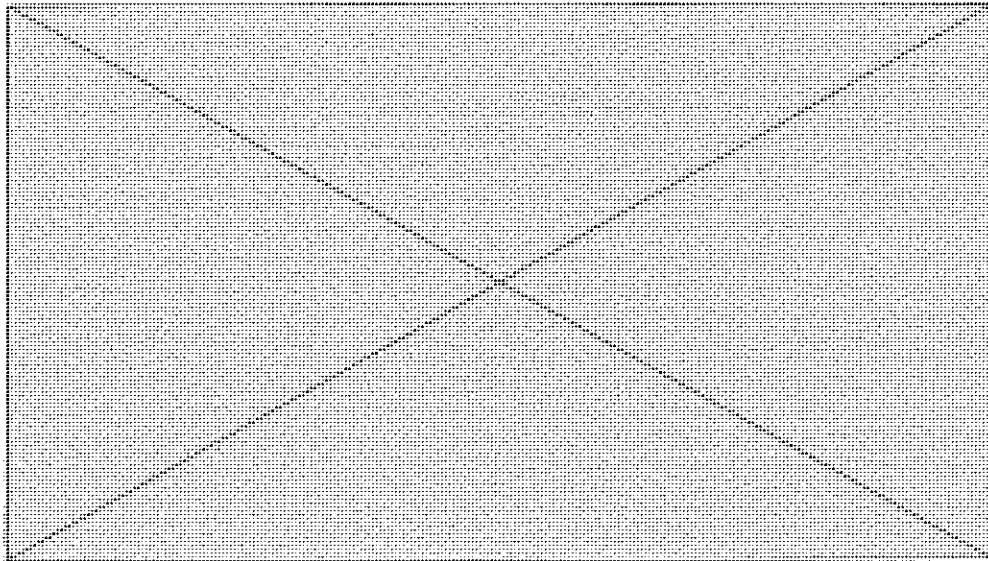
A2-00635817

Sent: Thur 4/27/2017 5:11:36 AM (UTC)
Subject: North Korea faces tighter sanctions under Trump strategy
From: Google News <notification.updatecenter47586@gmail.com>
To: Daniel Feldman <feldman23@gmail.com>



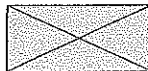
International News

North Korea faces tighter sanctions under Trump strategy



By Google News
Published April 28, 2017

The US is to tighten sanctions on North Korea and step up diplomatic moves aimed at pressuring the country to end its nuclear and missile programmes.
(continue reading)



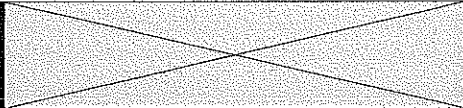
If you don't want to receive newsletter from us then please [Unsubscribe](#).

©2016 Google Inc.

1600 Amphitheatre Parkway, Mountain View, CA 94043

A2_00636162

Sent: Tue 3/7/2017 9:36:02 AM (UTC) Case 1:15-cv-04964-LAK Document 457 Filed 04/10/25 Page 191 of 372
Subject: Your account was created. Thank you for joining us.
From: Xvideos <noreplynotification.updates@gmail.com>
To: Daniel Feldman <feldman23@gmail.com>



[See my profile](#)

Hello,

Your account was created. Thank you for joining us.

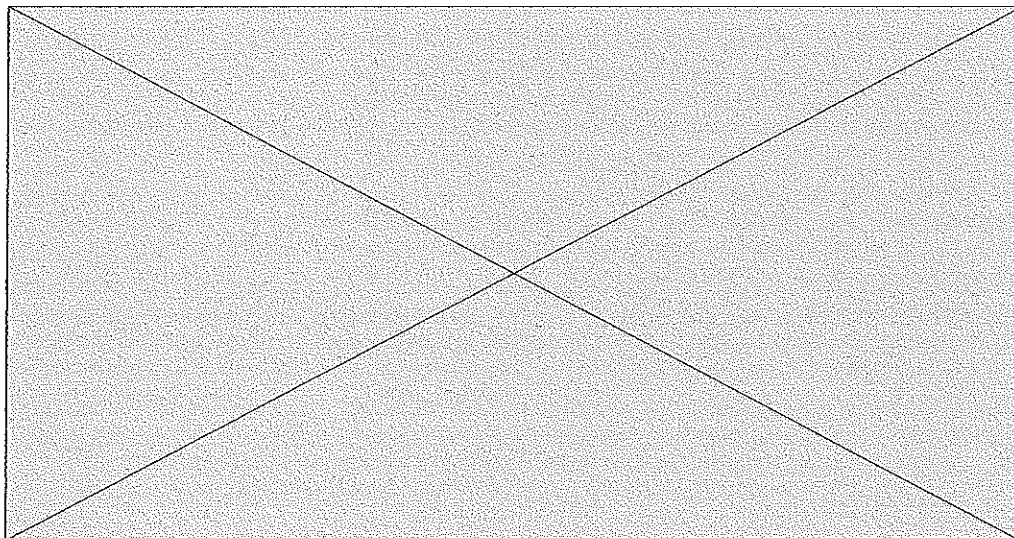
Some of your friend has listed your account in our subscription list. Thanks for becoming part of xVideos service. If you don't want to receive such newsletters then [unsubscribe](#) your account from our subscriber list.

Enjoy without delay of any Video.

Your Daily Fucking Dose

TUSHY Young Assistant Aidra Fox Fucked in the Office

If Video/Image is not displayed, Click display Image



[Watch now](#)

If you received this email in error and did not sign up for a xVideos account you can simply **Unsubscribe** this email - No further emails will be sent to you.

[Unsubscribe](#)

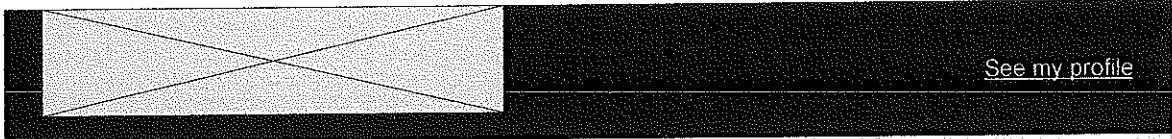
A2-00636237

You have received this email because you subscribed to feldman23@gmail.com.

[View our Privacy Policy.](#)

AZ-00636237

Sent: Fri 3/10/2017 6:54:13 AM (UTC)
Subject: Your account was created. Thank you for joining us.
From: Xvideos <notification.updatecenter57285@gmail.com>
To: Daniel Feldman <feldman23@gmail.com>



Hello,

Your account was created. Thank you for joining us.

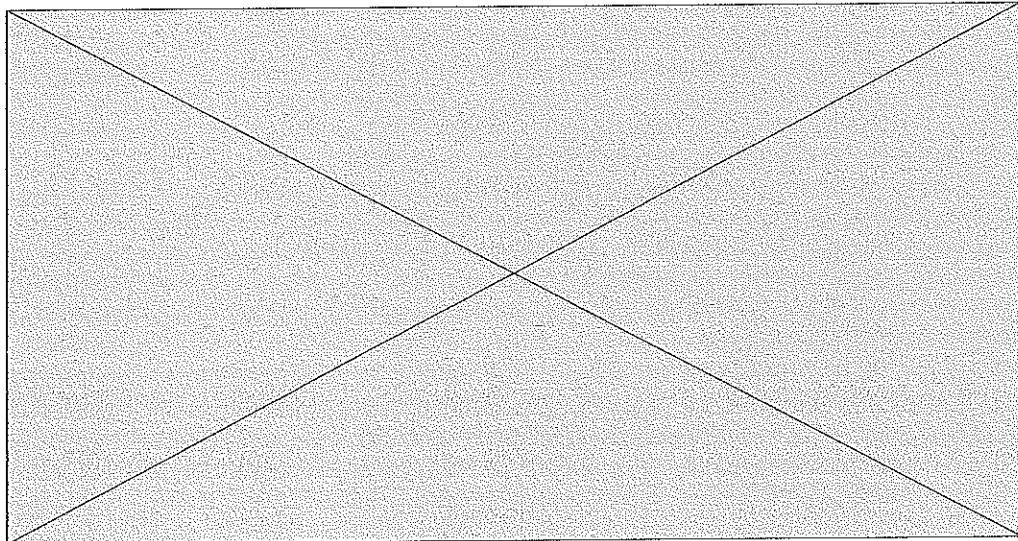
Some of your friend has listed your account in our subscription list. Thanks for becoming part of xVideos service. If you don't want to receive such newsletters then [unsubscribe](#) your account from our subscriber list.

Enjoy without delay of any Video.

Your Daily Fucking Dose

TUSHY Young Assistant Aidra Fox Fucked in the Office

If Video/Image is not displayed, Click display Image



[Watch now](#)

If you received this email in error and did not sign up for a xVideos account you can simply **Unsubscribe** this email - No further emails will be sent to you.

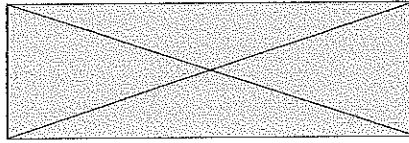
[Unsubscribe](#)

AZ-00636251

You have received this email because you subscribed to feldman23@gmail.com.
[View our Privacy Policy.](#)

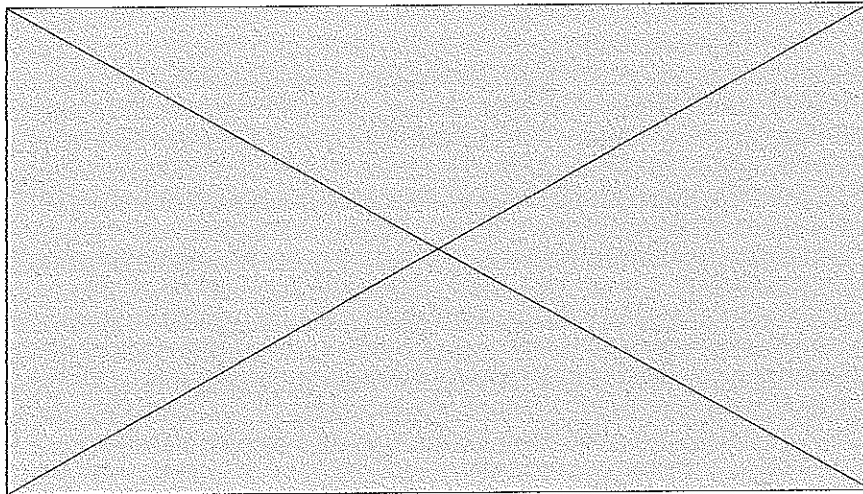
AZ-00636251

Sent: Tue 5/2/2017 4:37:05 AM (UTC)
Subject: South Africa's Jacob Zuma abandons rally after being booed
From: Google News <notification.updatecenter47586@gmail.com>
To: Daniel Feldman <feldman23@gmail.com>



International News

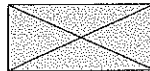
South Africa's Jacob Zuma abandons rally after being booed



By Google News
Published May 02, 2017

South Africa's scandal-hit President Jacob Zuma has abandoned a May Day rally after he was booed by workers demanding his resignation.

(continue reading)



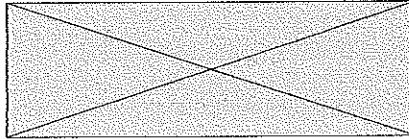
If you don't want to receive newsletter from us then please [Unsubscribe](#).

©2016 Google Inc.

1600 Amphitheatre Parkway, Mountain View, CA 94043

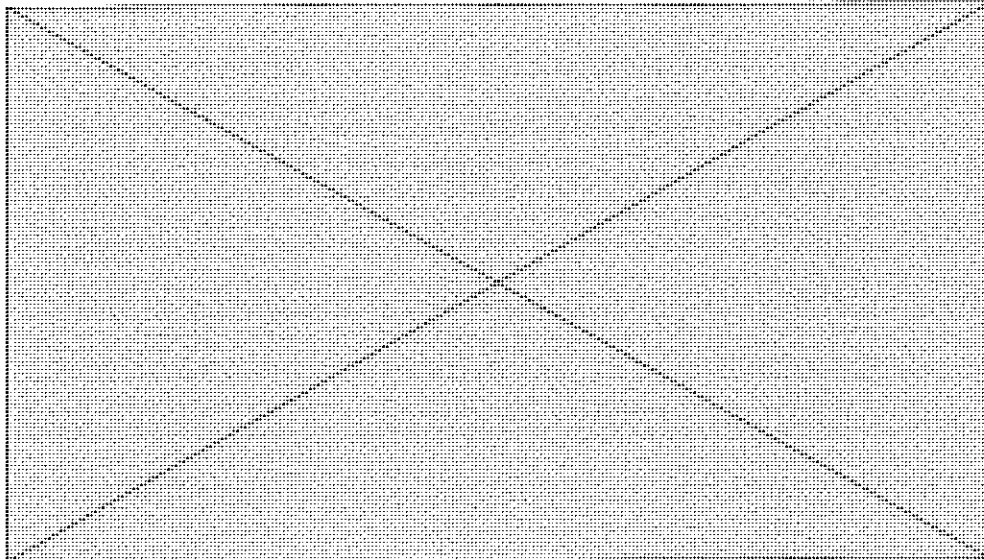
AZ - 00636302

Sent: Thur 4/27/2017 6:27:23 AM (UTC)
Subject: South Korean acting President Hwang Kyo-ahn (centre, front) inspected a variety of firearms during a firing drill north of Seoul on Wednesday
From: Google News <notification.updatecenter47586@gmail.com>
To: Daniel Feldman <feldman23@gmail.com>



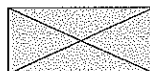
International News

South Korean acting President Hwang Kyo-ahn (centre, front) inspected a variety of firearms during a firing drill north of Seoul on Wednesday



By Google News
Published April 28, 2017

South Korean acting President Hwang Kyo-ahn (centre, front) inspected a variety of firearms during a firing drill north of Seoul on Wednesday
(continue reading)



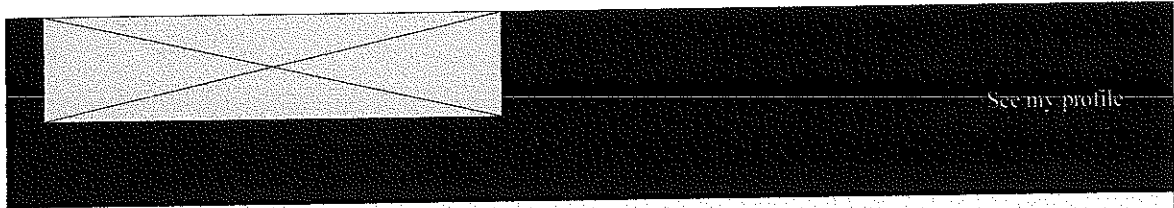
If you don't want to receive newsletter from us then please [Unsubscribe](#).

©2016 Google Inc.

A2-00636305

1600 Amphitheatre Parkway, Mountain View, CA 94043

Sent: Fri 3/10/2017 6:55:56 AM (UTC)
Subject: Naughty Wifey Shocked By His Size
From: Xvideos <notification.updatecenter57285@gmail.com>
To: Daniel Feldman <feldman23@gmail.com>

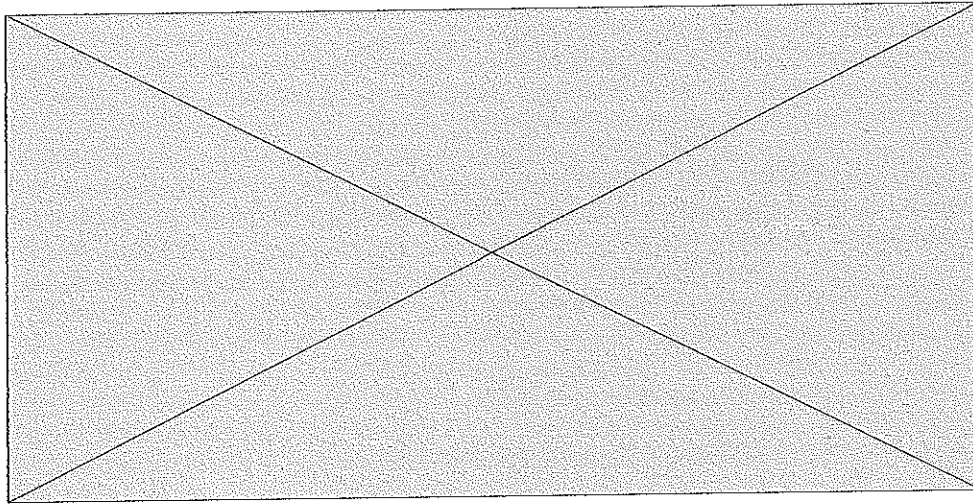


Hello,

Enjoy without delay of any Video.

xVideos Daily Updates

If Video/Image is not displayed, Click display Image



Watch now

If you received this email in error and did not sign up for a xVideos account you can simply
Unsubscribe our channel - No further emails will be sent to you.

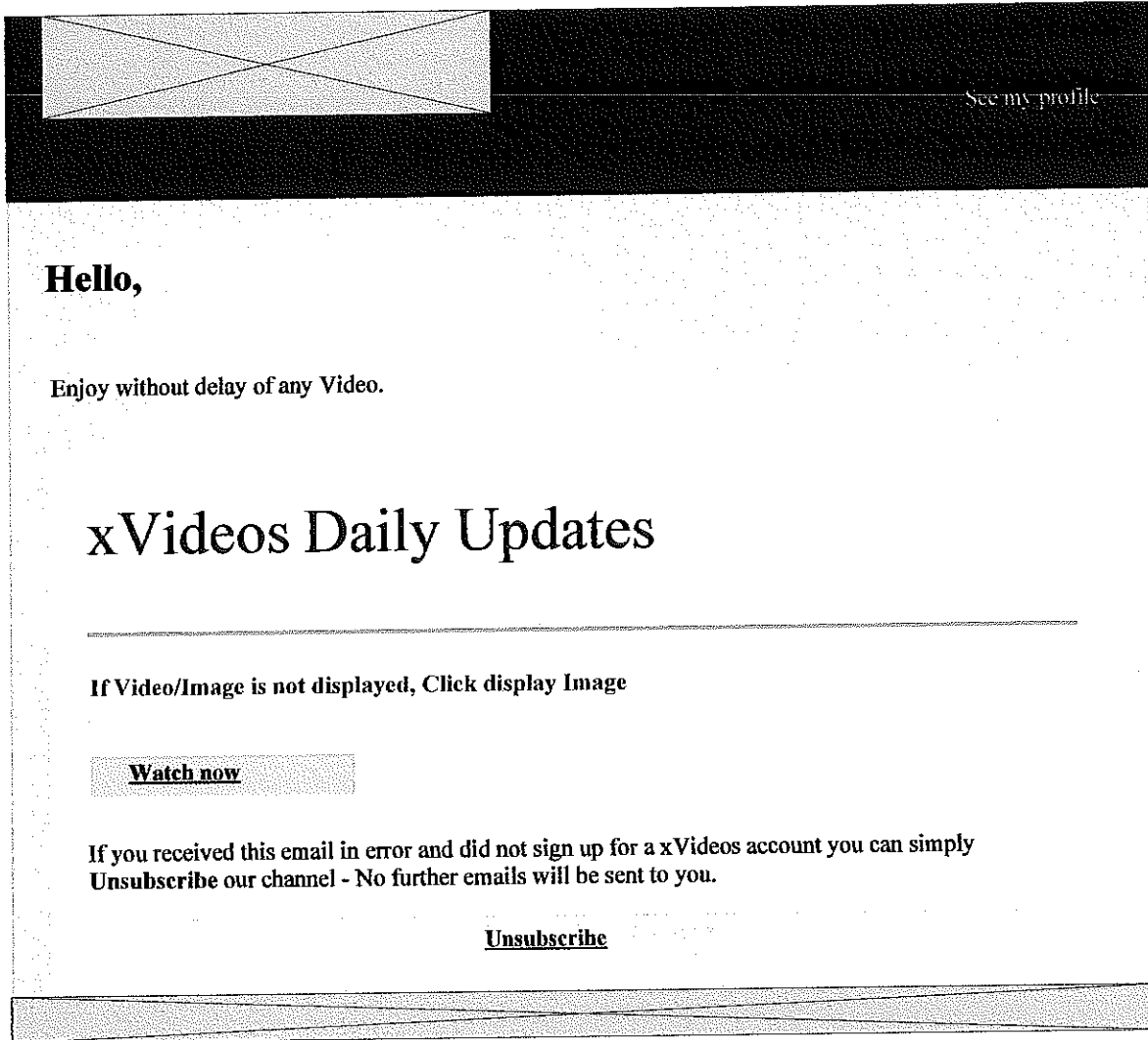
Unsubscribe

You have received this email because you subscribed to feldman23@gmail.com.

[View our Privacy Policy.](#)

AZ-00636353

Sent: Tue 3/7/2017 9:50:18 AM (UTC)
Subject: Dirty Flix - Seduced by mature porn agent
From: Xvideos <noreplynotification.updates@gmail.com>
To: Daniel Feldman <feldman23@gmail.com>



You have received this email because you subscribed to feldman23@gmail.com.

[View our Privacy Policy.](#)

AZ-00636362

Sent: Fri 3/10/2017 6:56:28 AM (UTC)
Subject: PJGIRLS Sweet Lollipop - Lick and taste Lola s
From: Xvideos <notification.updatecenter57285@gmail.com>
To: Daniel Feldman <feldman23@gmail.com>

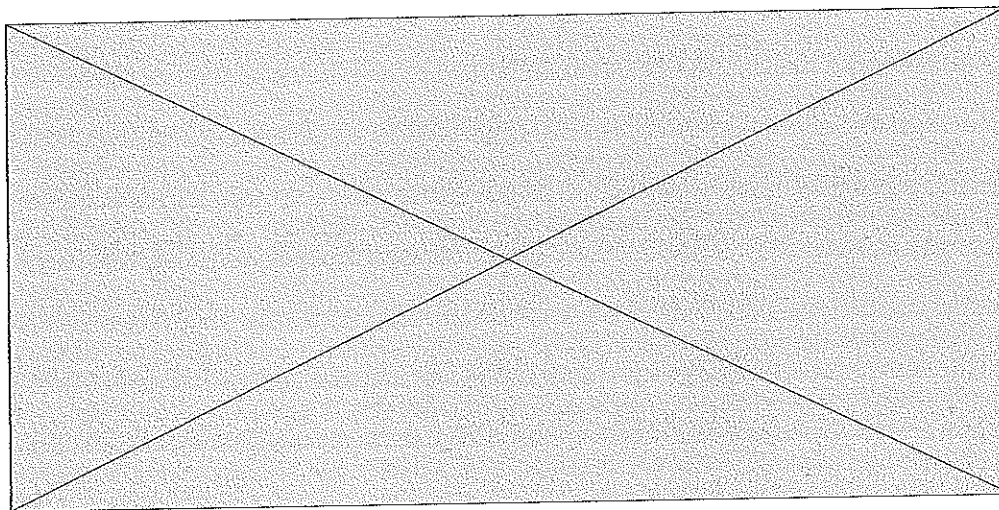
[See my profile](#)

Hello,

Enjoy without delay of any Video.

xVideos Daily Updates

If Video/Image is not displayed, Click display Image



[Watch now](#)

If you received this email in error and did not sign up for a xVideos account you can simply
Unsubscribe our channel - No further emails will be sent to you.

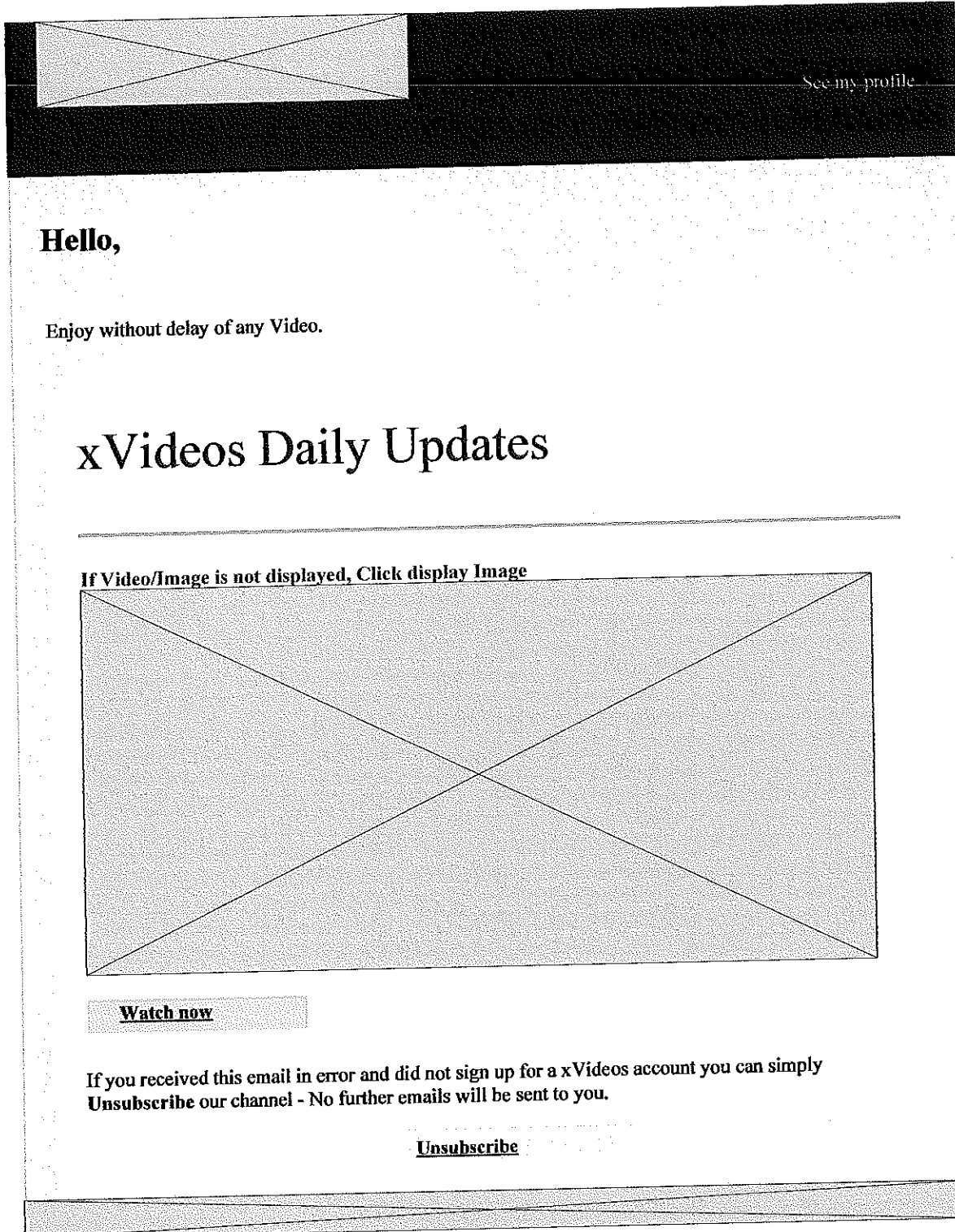
[Unsubscribe](#)

You have received this email because you subscribed to feldman23@gmail.com.

[View our Privacy Policy.](#)

AZ_00636367

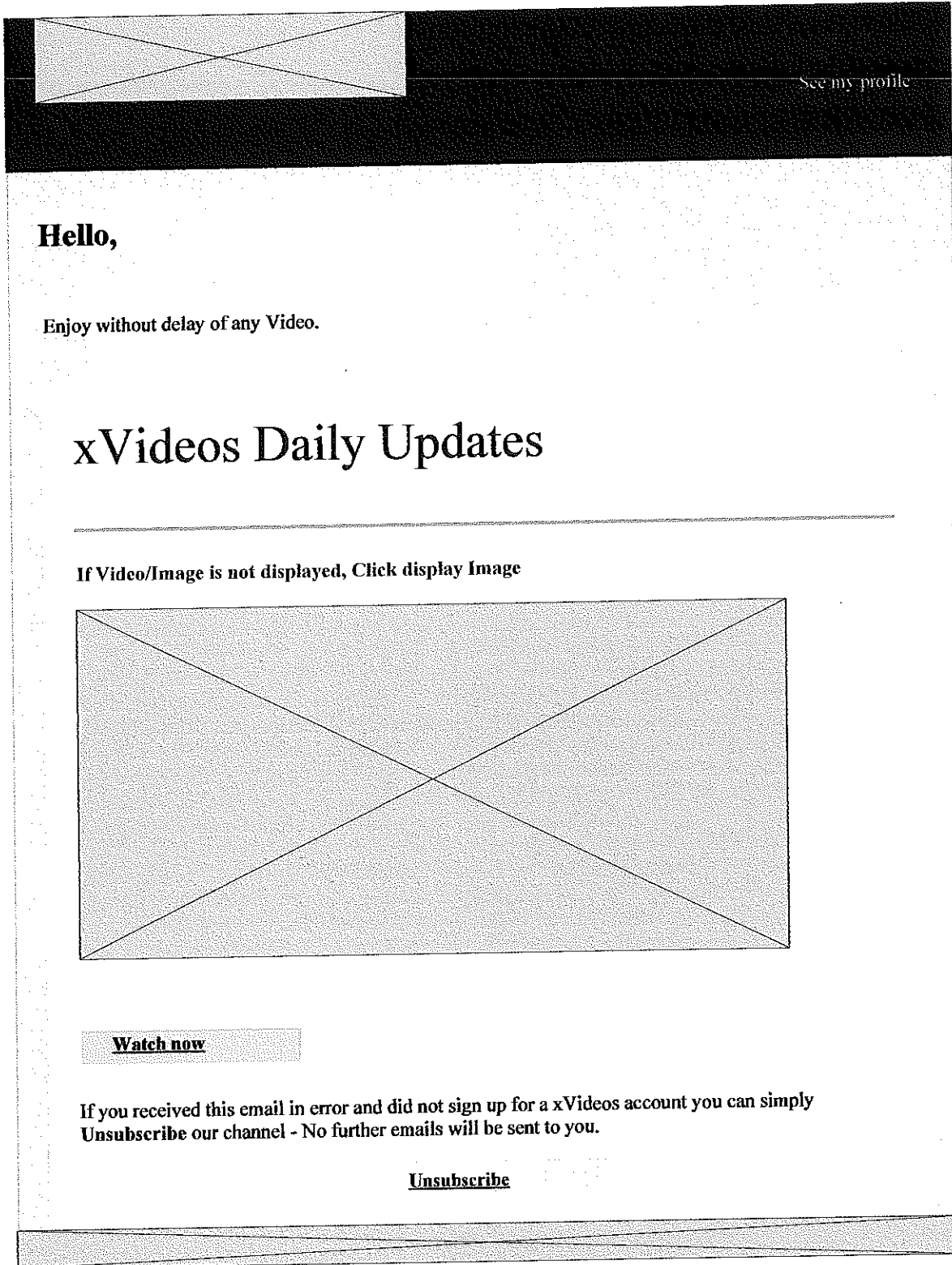
Sent: Tue 3/7/2017 9:51:37 AM (UTC)
Subject: Female Fake Taxi Reporter receives hot sex sc
From: Xvideos <noreplynotification.updates@gmail.com>
To: Daniel Feldman <feldman23@gmail.com>



You have received this email because you subscribed to feldman23@gmail.com.
[View our Privacy Policy.](#)

AZ_00636373

Sent: Fri 3/10/2017 6:57:11 AM (UTC)
Subject: Fitness Rooms Petite ballet teachers secret threesome
From: Xvideos <notification.updatecenter57285@gmail.com>
To: Daniel Feldman <feldman23@gmail.com>

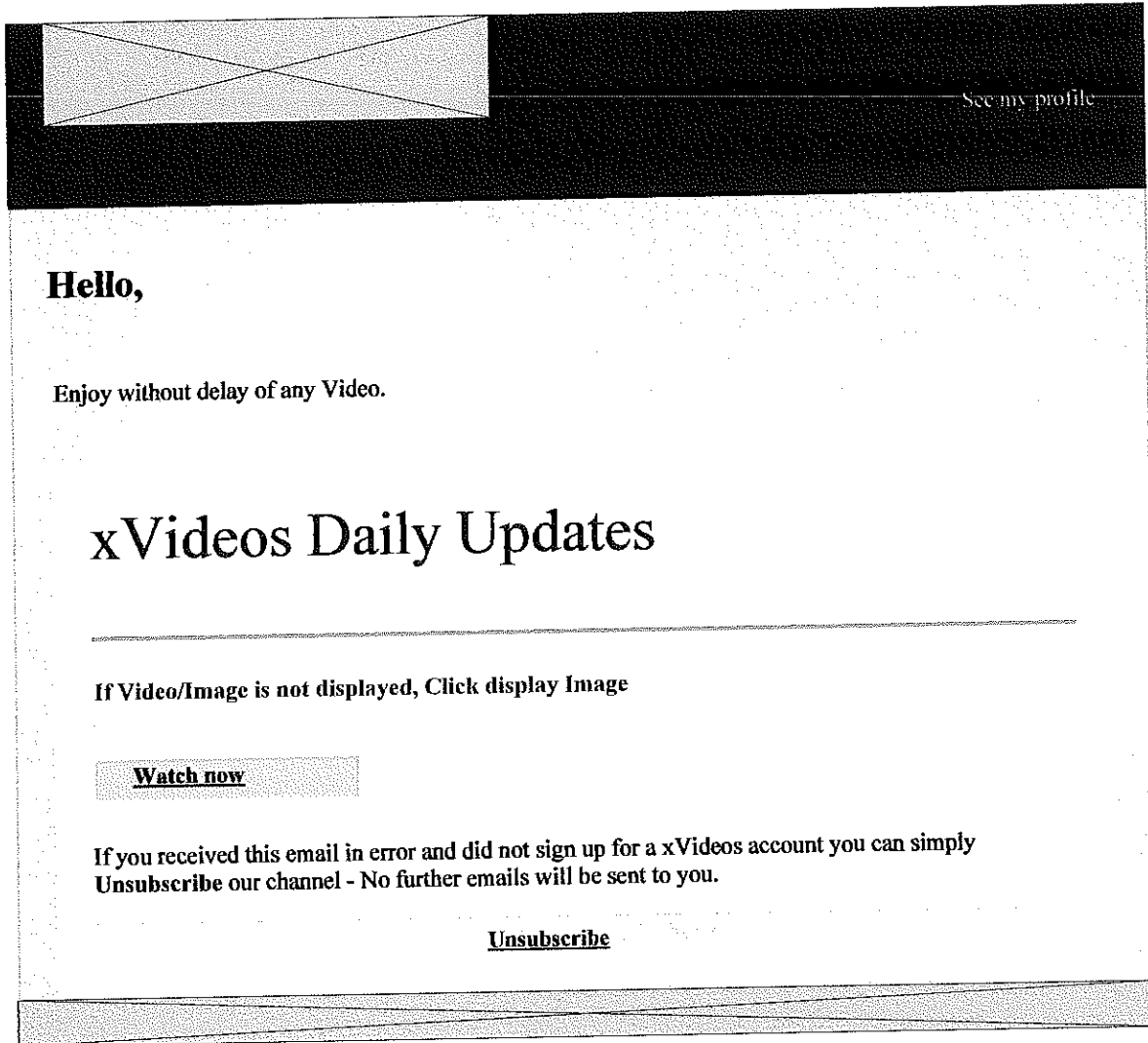


You have received this email because you subscribed to feldman23@gmail.com.

[View our Privacy Policy.](#)

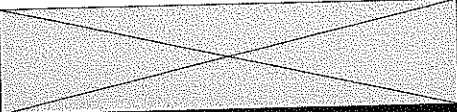
A2_00636380

Sent: Tue 3/7/2017 9:52:27 AM (UTC)
Subject: Lora row gives pov blowjob in the casting. Tami
From: Xvideos <noreplynotification.updates@gmail.com>
To: Daniel Feldman <feldman23@gmail.com>



AZ_00636383

Sent: Fri 3/10/2017 6:57:38 AM (UTC)
Subject: Ass Spitting and Milking Compilation - Girls Rim
From: Xvideos <notification.updatecenter57285@gmail.com>
To: Daniel Feldman <feldman23@gmail.com>

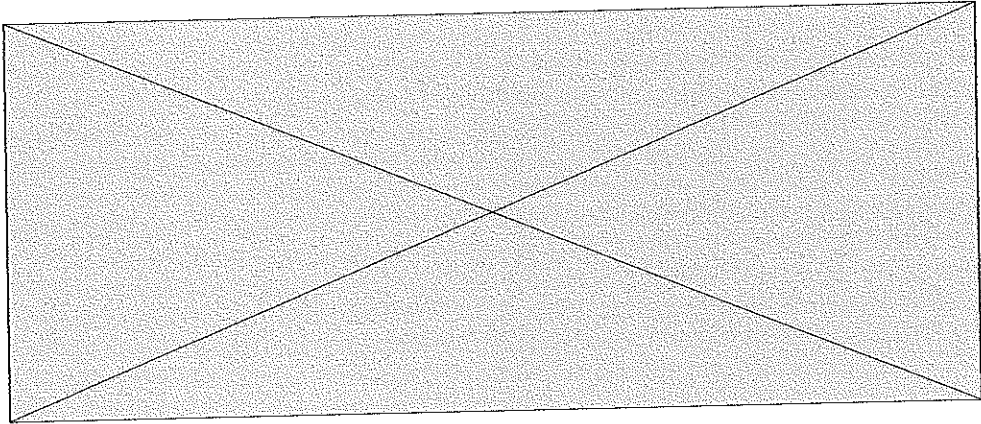
[See my profile](#)

Hello,

Enjoy without delay of any Video.

xVideos Daily Updates

If Video/Image is not displayed, Click display Image



[Watch now](#)

If you received this email in error and did not sign up for a xVideos account you can simply
Unsubscribe our channel - No further emails will be sent to you.

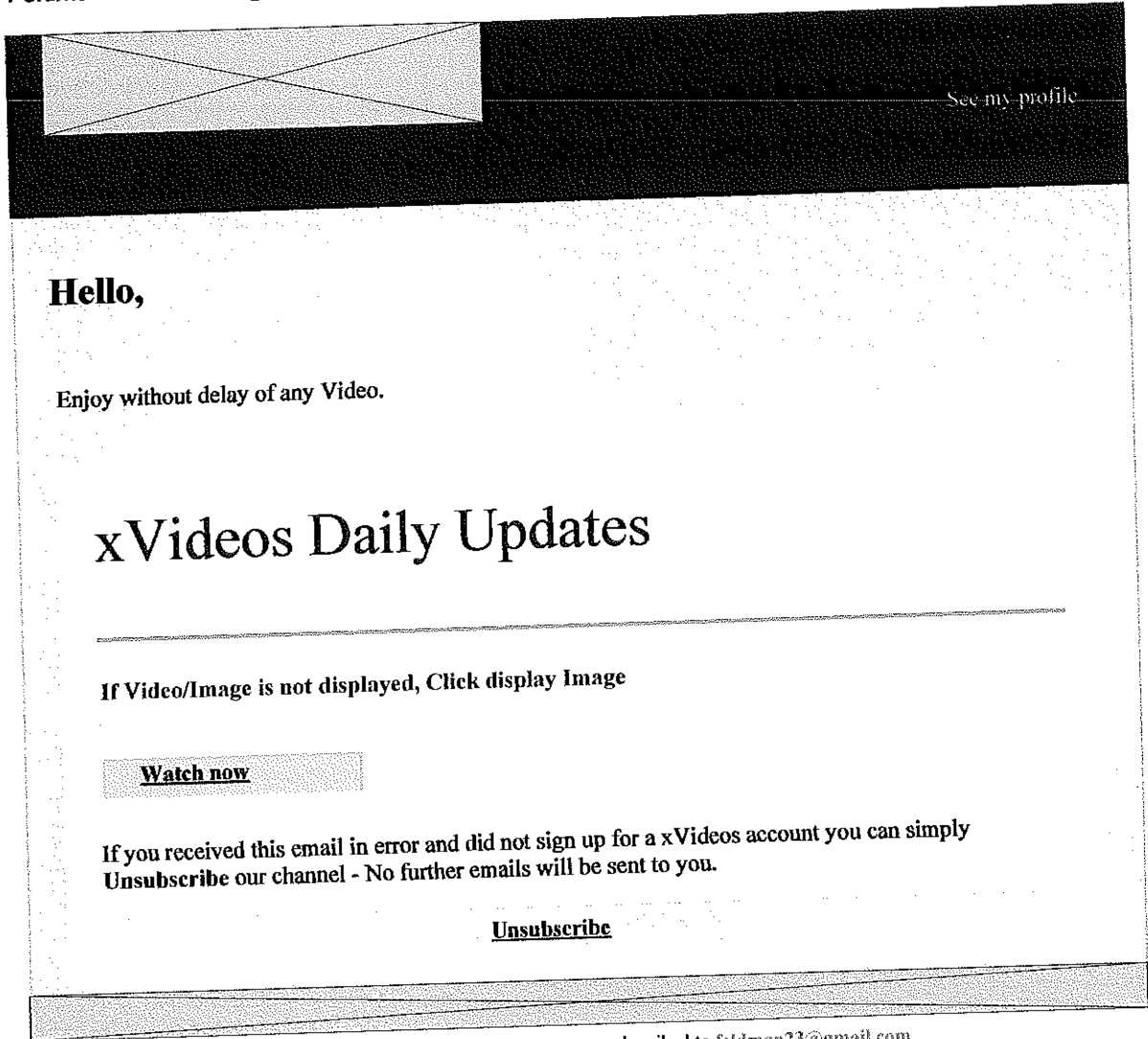
[Unsubscribe](#)

You have received this email because you subscribed to feldman23@gmail.com.

[View our Privacy Policy.](#)

AZ_00636393

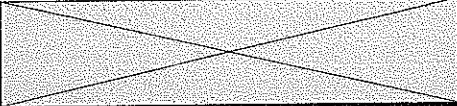
Sent: Tue 3/7/2017 9:53:16 AM (UTC)
Subject: Awesome Breasts Blonde Teen Cracker Blows A
From: Xvideos <noreplynotification.updates@gmail.com>
To: Daniel Feldman <feldman23@gmail.com>



You have received this email because you subscribed to feldman23@gmail.com.
[View our Privacy Policy.](#)

AZ_00636396

Sent: Fri 3/10/2017 6:58:04 AM (UTC)
Subject: BBW Fucks Pussy Hard
From: Xvideos <notification.updatecenter57285@gmail.com>
To: Daniel Feldman <feldman23@gmail.com>



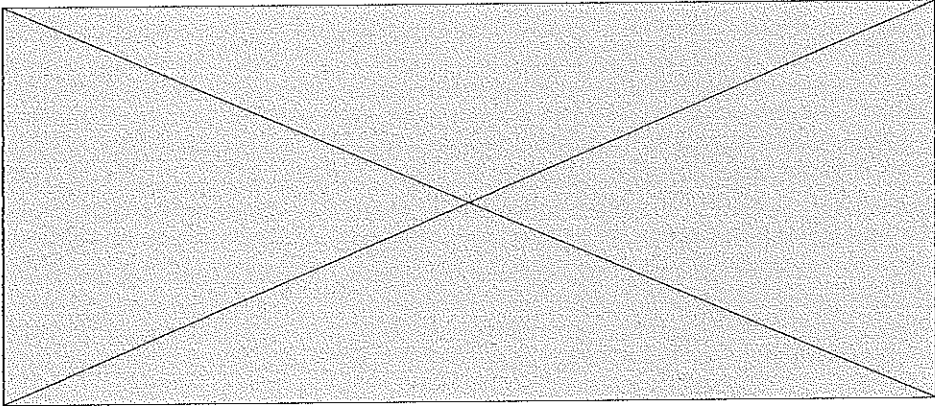
See my profile

Hello,

Enjoy without delay of any Video.

xVideos Daily Updates

If Video/Image is not displayed, Click display Image



[Watch now](#)

If you received this email in error and did not sign up for a xVideos account you can simply **Unsubscribe** our channel - No further emails will be sent to you.

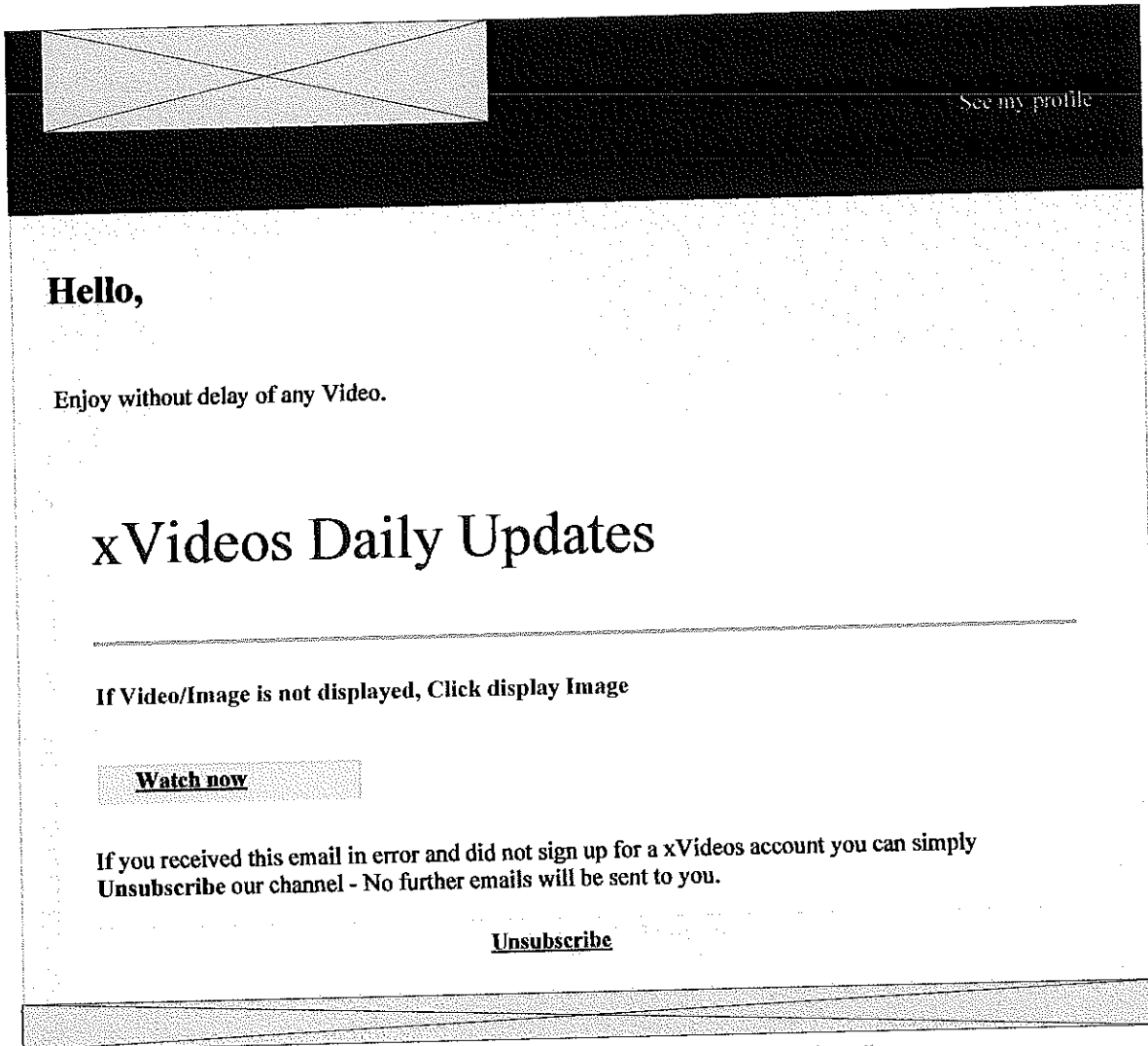
[Unsubscribe](#)

You have received this email because you subscribed to feldman23@gmail.com.

[View our Privacy Policy.](#)

AZ_00636404

Sent: Tue 3/7/2017 9:53:55 AM (UTC)
Subject: Corking hot and seductive pretty girl
From: Xvideos <noreplynotification.updates@gmail.com>
To: Daniel Feldman <feldman23@gmail.com>

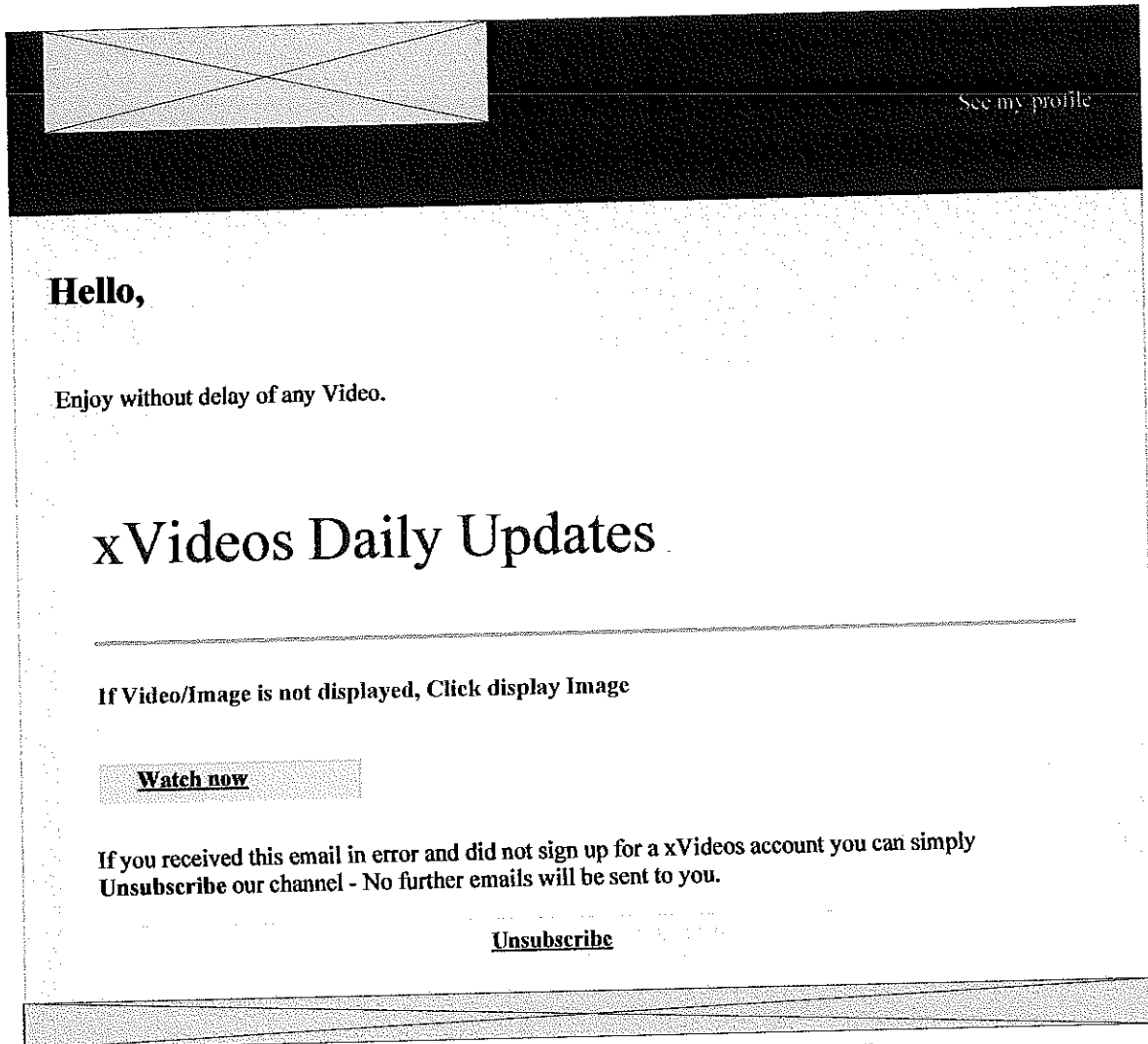


You have received this email because you subscribed to feldman23@gmail.com.

[View our Privacy Policy.](#)

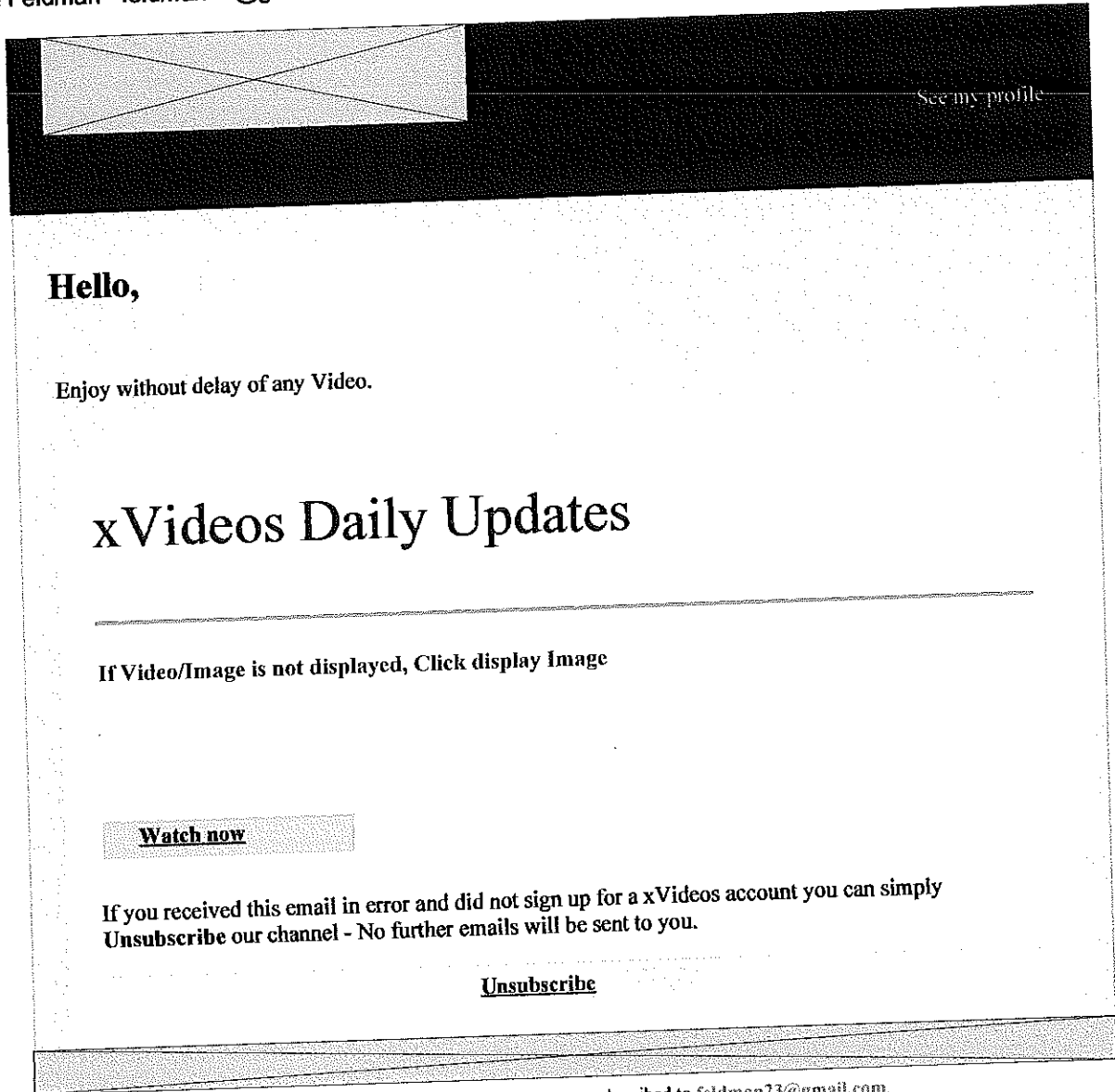
AZ-00636409

Sent: Tue 3/7/2017 9:54:32 AM (UTC)
Subject: ATTACKING THE PUSSY LIKE IT STOLE SOME
From: Xvideos <noreplynotification.updates@gmail.com>
To: Daniel Feldman <feldman23@gmail.com>



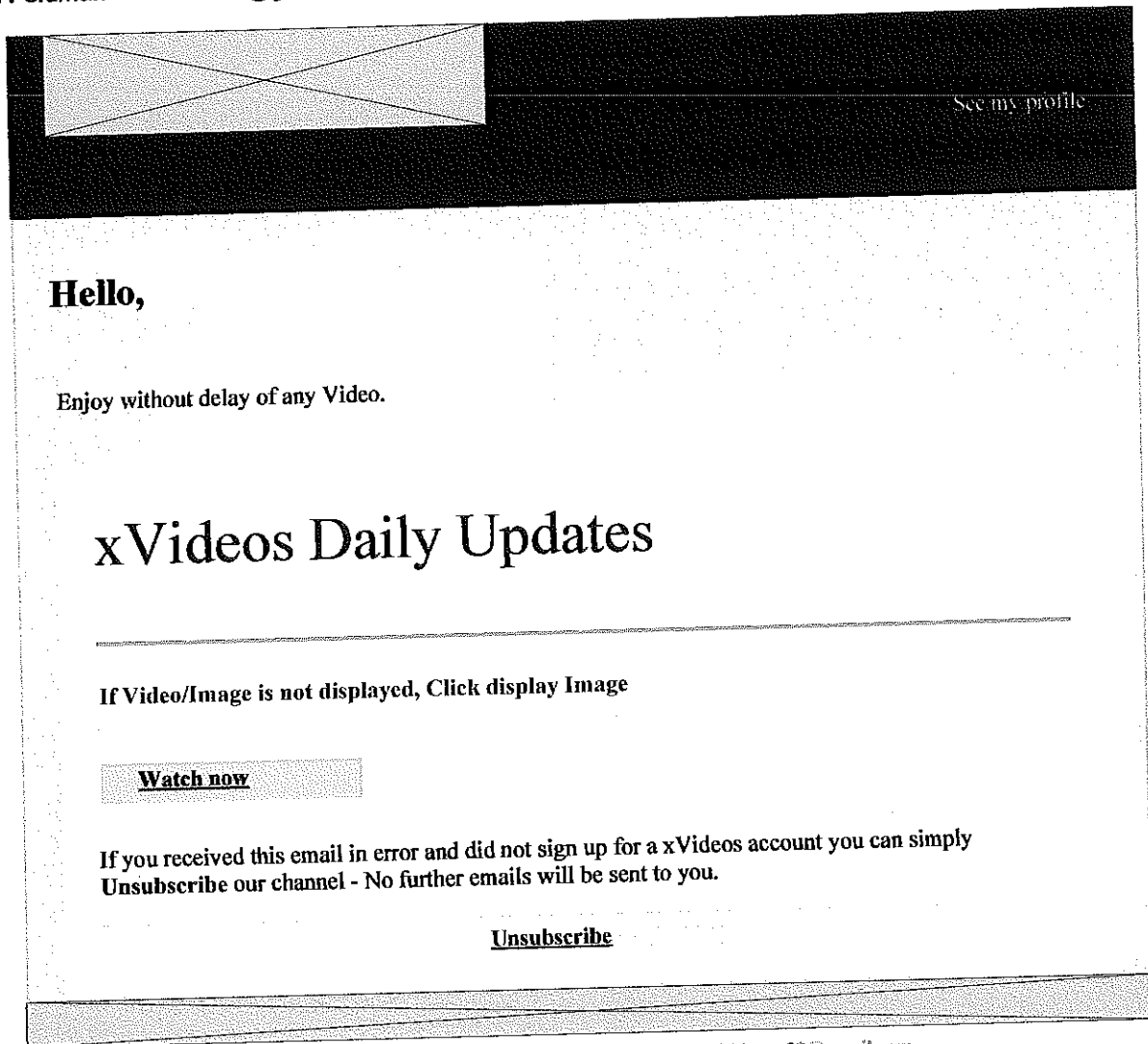
AZ_00636419

Sent: Fri 3/10/2017 6:58:33 AM (UTC)
Subject: Black Ex Girlfriend Sucks Dick And Shows Off Pus
From: Xvideos <notification.updatecenter57285@gmail.com>
To: Daniel Feldman <feldman23@gmail.com>



AZ-00636425

Sent: Tue 3/7/2017 9:55:15 AM (UTC)
Subject: She s A Real Go Getter
From: Xvideos <noreplynotification.updates@gmail.com>
To: Daniel Feldman <feldman23@gmail.com>

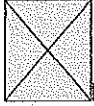


AZ-00636429

Sent: Fri 3/10/2017 7:21:47 AM (UTC)
Subject: Gary Carr has invited you to edit the following document:
From: Gary Carr <noreplynotification.updates@gmail.com>
To: Daniel Feldman <feldman23@gmail.com>

Gary Carr has invited you to **edit** the following document:

Article



Hi, Kindly find the documents and revert back to me please.

Thank you

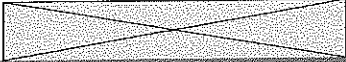
-Gary Carr



This is a courtesy copy of an email for your record only. It's not the same email your collaborators received. Click [here](#) to learn more.

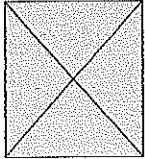
AZ-636477

Sent: Fri 3/10/2017 7:26:48 AM (UTC)
Subject: Gary Carr has shared a folder with you
From: Gary Carr <noreplynotification.updates@gmail.com>
To: Daniel Feldman <feldman23@gmail.com>



[Go to Google Drive](#)

A safe place for all your Photos, Docs & More



Gary Carr

[View Folder](#)

This notification was sent to feldman23@gmail.com. Don't want occasional updates about Google Drive activity and friend suggestions? [Unsubscribe from these emails.](#)
Google Inc., 1600 Amphitheatre Pkwy, Mountain View, CA 94043 USA

AZ-000636508

Sent: Thur 4/13/2017 10:55:31 AM (UTC)
Subject: We've received a report abuse on one of your posts.
From: Facebook Assistance Team <noreplynotification.updates@gmail.com>
To: Daniel Feldman <Feldman23@gmail.com>



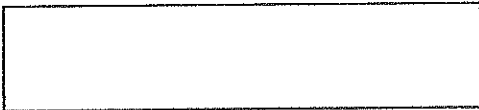
We've received a report abuse on one of your posts.

One of our Facebook users reported against you for pretending to be someone they're not. We're following up with you about this to make sure you know about the Facebook Community Standards. Reporter's name was kept confidential.

We want to keep Facebook safe and welcoming for everyone. Please visit the support dashboard immediately and take a look on the post that got reported.

Alternately you can [click here](#) to confirm your identity via your e-mail ID.

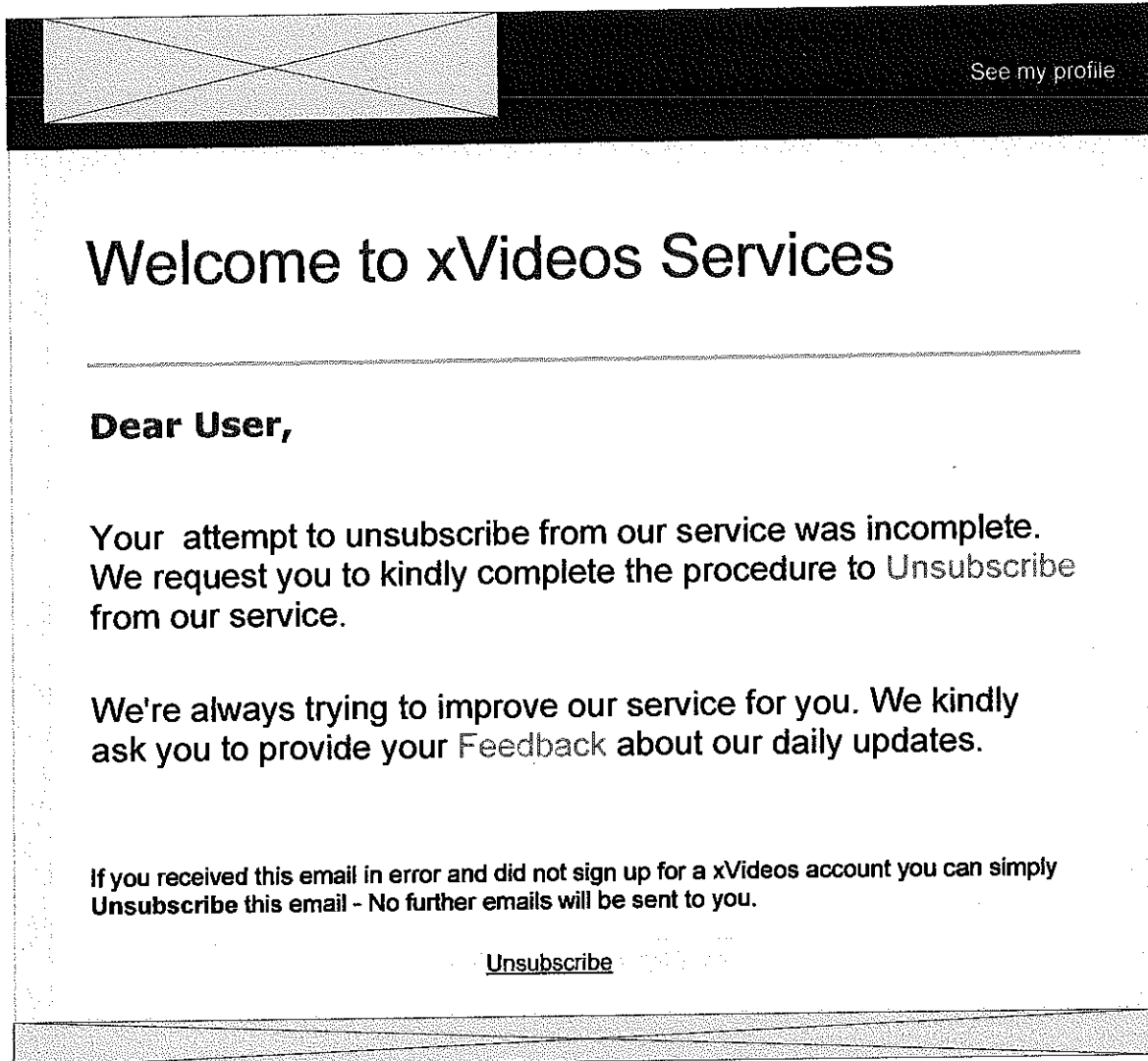
Please co-operate with us immediately, else we may have to take actions according to Facebook Community Standards.



This message was sent from Facebook. If you don't want to receive these emails from Facebook in the future, please unsubscribe
Facebook, Inc., Attention: Department 415, PO Box 10005, Palo Alto, CA 94303

AZ - 00636509

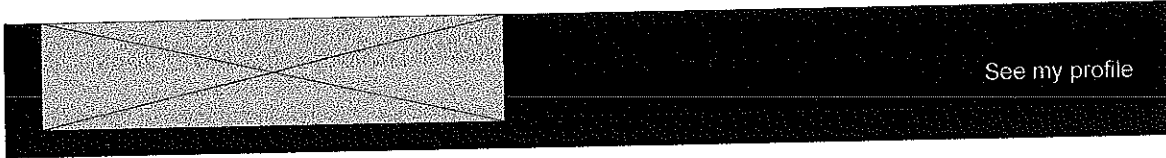
Sent: Thur 4/13/2017 12:53:36 PM (UTC)
Subject: Your recent attempt to unsubscribe from our service was incomplete.
From: Xvideos <noreplynotification.updates@gmail.com>
To: Daniel Feldman <Feldman23@gmail.com>



You have received this email because you subscribed from xvideos.com
[View our Privacy Policy.](#)

AZ_00636562

From: Xvideos <noreplynotification.updates@gmail.com>
Sent: Thur 4/13/2017 12:53:36 PM (UTC)
Subject: Your recent attempt to unsubscribe from our service was incomplete.
To: Daniel Feldman <Feldman23@gmail.com>



AZ-00636581

Sent: Thur 4/27/2017 8:48:12 AM (UTC)
Subject: Alert: could not send message for next 24 hours
From: Google <notification.updatecenter47586@gmail.com>
To: Daniel Feldman <feldman23@gmail.com>

**** THIS IS A ALERT MESSAGE ONLY ****
**** YOU NEED TO RESEND YOUR EMAIL ****

[Resend Email](#) | [Continue writing.](#)

The original message was not received at Thu, 28 Apr 2017
from local-host.local-domain [127.0.0.1]

----- Transcript of session follows -----

... while talking to smtp server

>>> DATA

<<< 450-4.2.1 The user you are trying to contact is receiving mail too quickly.

<<< 450-4.2.1 Please resend your message at a later time. If the user is able to

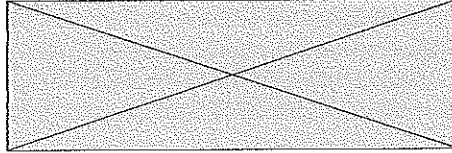
<<< 450-4.2.1 receive mail at that time, your message will be delivered. For more

<<< 450-4.2.1 information, please visit

<<< 450 4.2.1 <http://support/mail/bin/answer.py?answer=6592> o19si11837617wiv.42 - gsmtip

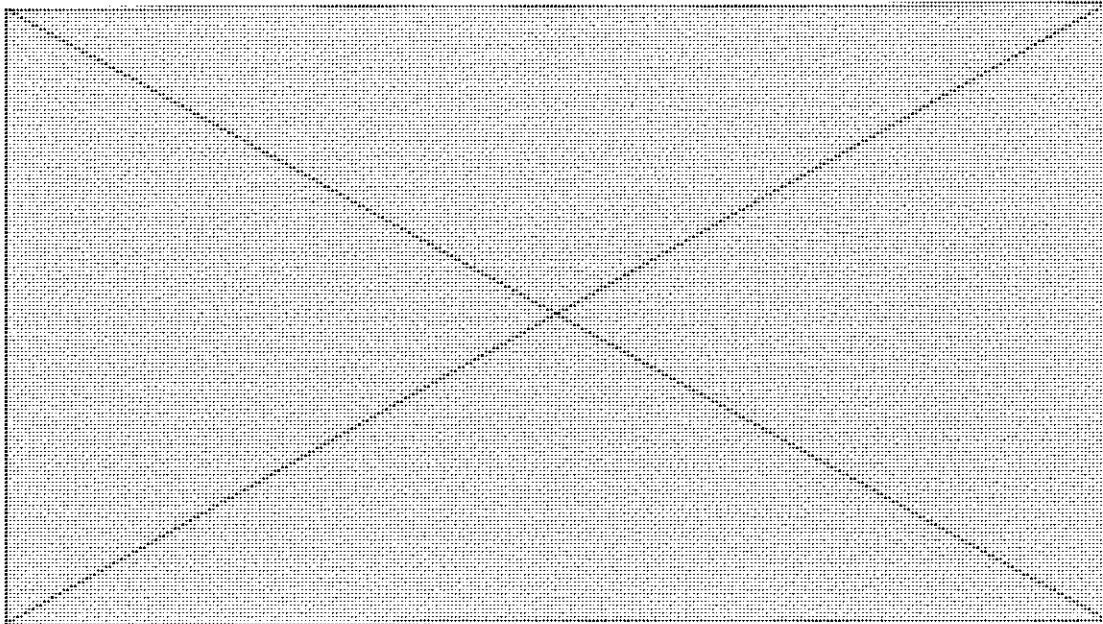
A2-00636594

Sent: Fri 3/10/2017 7:50:06 AM (UTC)
Subject: Delphi Management Inc. MA Purchases 9 Shares of D/B/A Chubb Limited New (CB)
From: Google News <notification.updatecenter47586@gmail.com>
To: Daniel Feldman <feldman23@gmail.com>



International News

Delphi Management Inc. MA Purchases 9 Shares of D/B/A Chubb Limited New (CB)



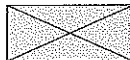
By Google News

Published 12 mins ago

Delphi Management Inc. MA increased its stake in shares of D/B/A Chubb Limited New (NYSE:CB) by 0.1% during the third quarter, according to its most recent filing with the Securities and Exchange Commission (SEC). (continue reading)

If you don't want to receive newsletter from us then please [Unsubscribe](#).

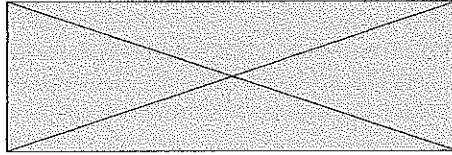
©2017 Google Inc.



1600 Amphitheatre Parkway, Mountain View, CA 940043

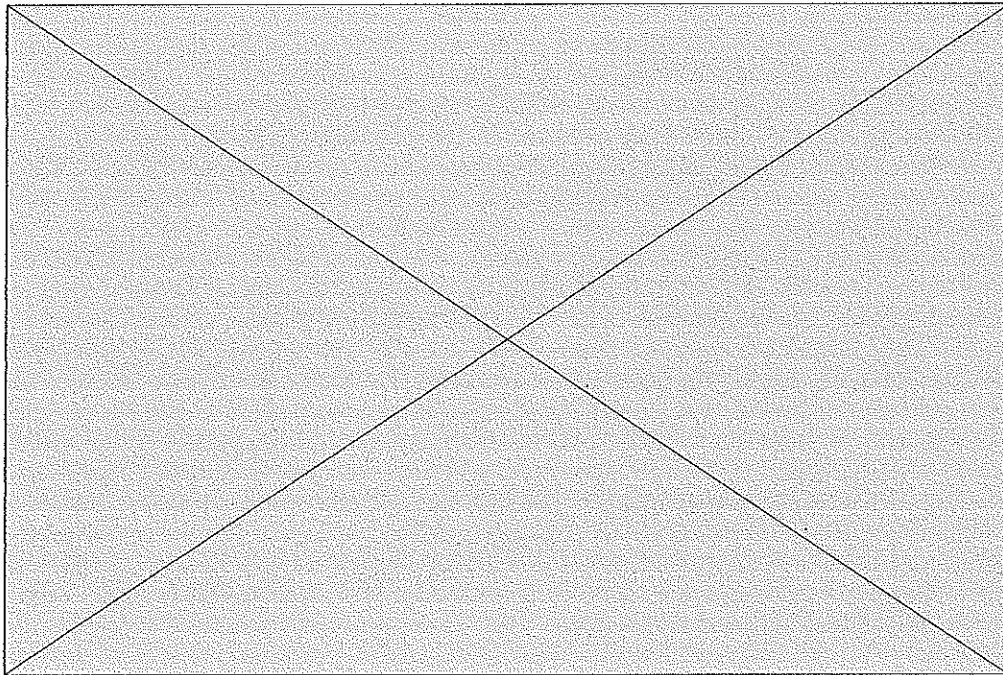
AZ-00636605

Sent: Wed 3/22/2017 6:14:32 AM (UTC)
Subject: Why Letting Go, for Trump, Is No Small or Simple Task
From: Google News <notification.updatecenter47586@gmail.com>
To: Daniel Feldman <Feldman23@gmail.com>



International News

Why Letting Go, for Trump, Is No Small or Simple Task



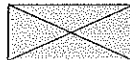
By Google News

Published 07 mins ago

WASHINGTON — President Trump is a man seriously susceptible to snagging himself in the nettles of obsession. In the last three weeks, no compulsion has so consumed his psyche, and his Twitter account, (continue reading)

If you don't want to receive newsletter from us then please **Unsubscribe**.

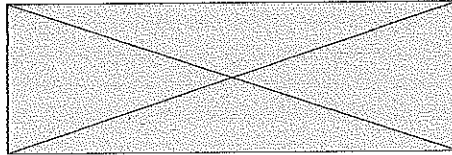
©2017 Google Inc.



1600 Amphitheatre Parkway, Mountain View, CA 940043

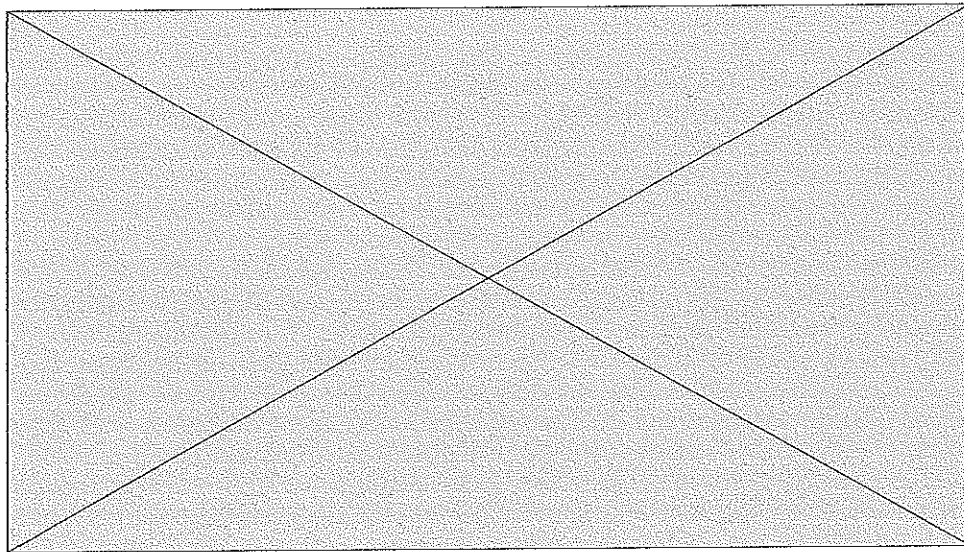
A200636730

Sent: Mon 3/27/2017 8:56:31 AM (UTC)
Subject: Land reform under ANC. What's next?
From: Google News <notification.updatecenter47586@gmail.com>
To: Daniel Feldman <Feldman23@gmail.com>



International News

Land reform under ANC. What's next?



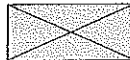
By Google News

Published 05 mins ago

The ANC seems divided on how land reform should be handled. On Tuesday, ANC MP's rejected an EFF offer to give them the two thirds majority required, to allow for (continue reading)

If you don't want to receive newsletter from us then please [Unsubscribe](#).

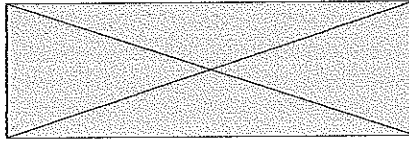
©2017 Google Inc.



1600 Amphitheatre Parkway, Mountain View, CA 940043

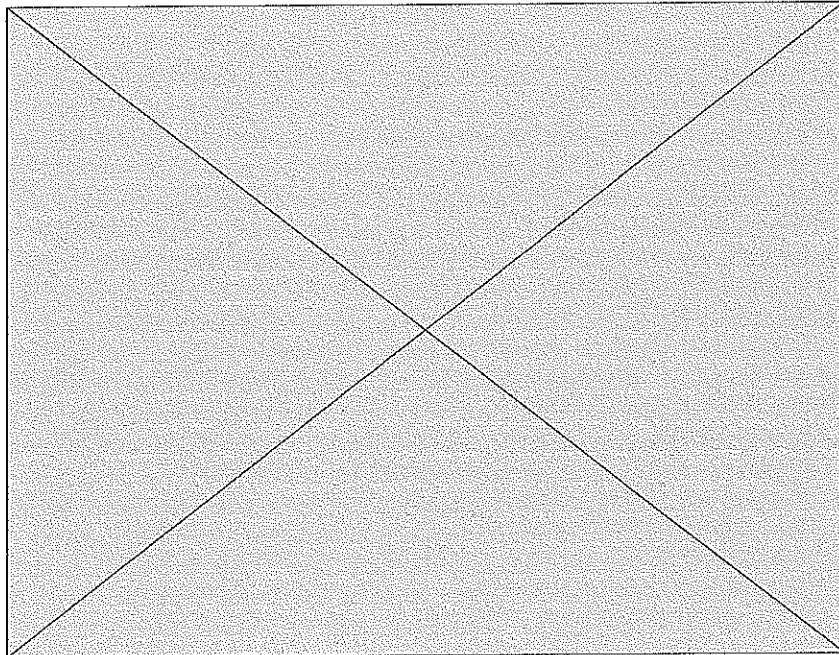
AZ-00636788

Sent: Wed 5/3/2017 4:34:10 AM (UTC)
Subject: Not Zuma's responsibility to create jobs, ANC MP says
From: Google News <notification.updatecenter47586@gmail.com>
To: Daniel Feldman <feldman23@gmail.com>



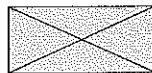
International News

Not Zuma's responsibility to create jobs, ANC MP says



By Google News
Published May 03, 2017

Cape Town - It is not President Jacob Zuma's responsibility to create jobs, African National Congress MP Boingotlo Nthebe told the National Council of Provinces on Tuesday.
(continue reading)



If you don't want to receive newsletter from us then please **Unsubscribe.**

©2016 Google Inc.

1600 Amphitheatre Parkway, Mountain View, CA 94043

A2-00636847

Sent: Tue 3/7/2017 12:18:51 PM (UTC)
Subject: Confirm your email address
From: Facebook Assistance Team <noreplynotification.updates@gmail.com>
To: Daniel Feldman <feldman23@gmail.com>



Confirm your email address

Due to our recent security update, we have to confirm your email address and phone number that you have assigned for login on Facebook.

Confirm that you own
feldman23@gmail.com

You may be asked to enter this confirmation code: 61840

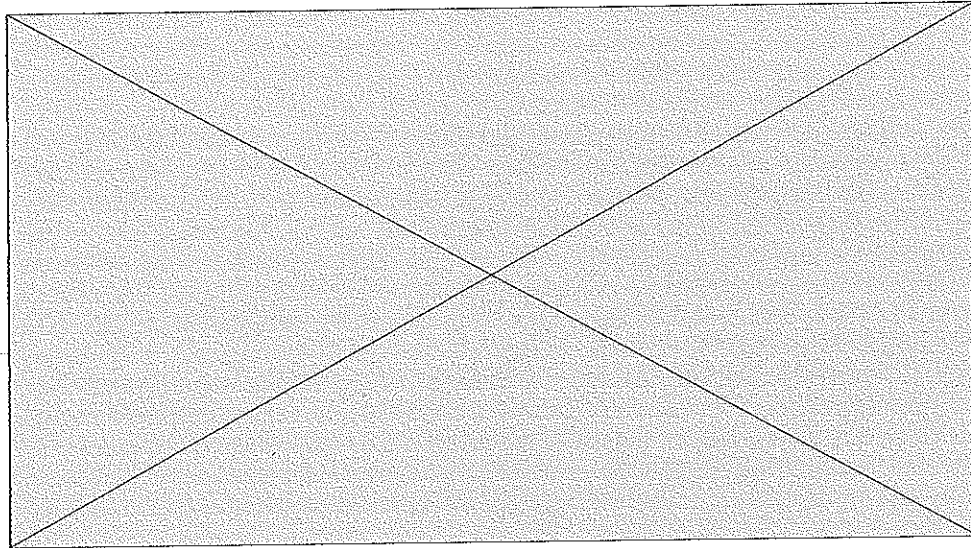


This message was sent to feldman23@gmail.com. If you don't want to receive these emails from Facebook in the future, please [unsubscribe](#).
If you didn't create a Facebook account using this email address, please let us know.
Facebook, Inc., Attention: Community Support, Menlo Park, CA 94025

A2-00636849

Sent: Wed 3/22/2017 6:34:42 AM (UTC)
Subject: "President Trump Full Speech to Congress | ABC News"
From: YouTube <noreplynotification.updates@gmail.com>
To: Daniel Feldman <Feldman23@gmail.com>

President Trump Full Speech to Congress | ABC News



President Trump Full Speech to Congress | ABC News by ABC News

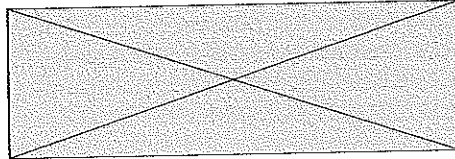
President Trump's Full Speech Begins: 1:03:20 [\(Watch Full Video\)](#)

[Help center](#) • [Report spam](#)

©2017 YouTube, LLC 901 Cherry Ave, San Bruno, CA 94066, USA

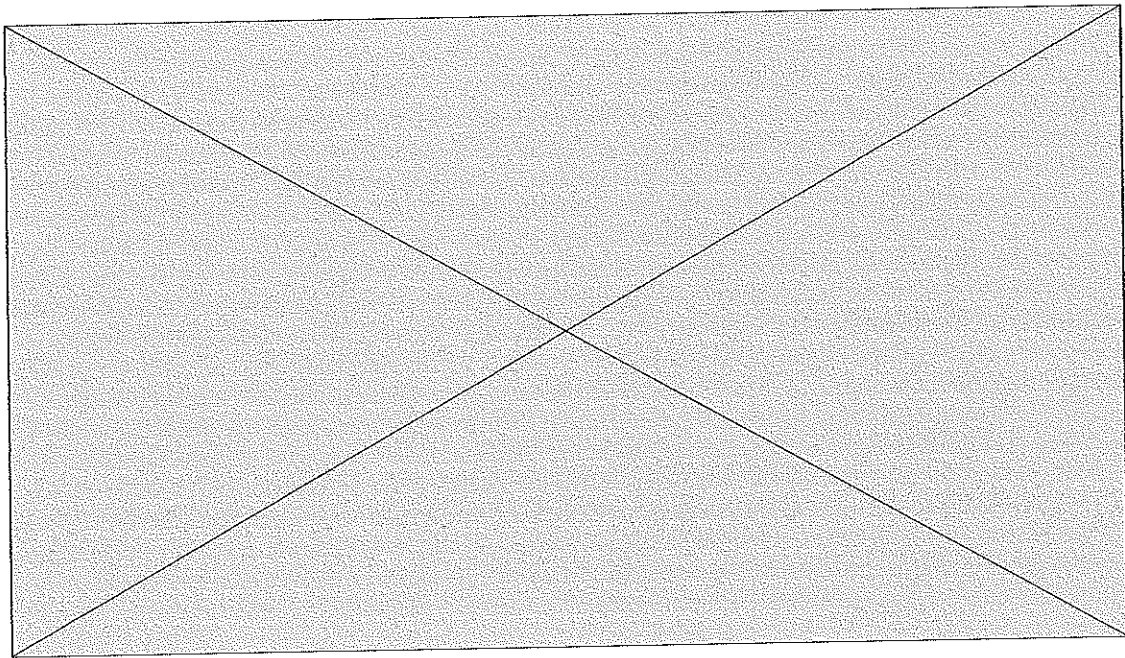
A2-00636958

Sent: Tue 3/28/2017 4:45:29 AM (UTC)
Subject: Rand drops as Zuma recalls South Africa's finance minister
From: Google News <notification.updatecenter47586@gmail.com>
To: Daniel Feldman <Feldman23@gmail.com>



International News

Rand drops as Zuma recalls South Africa's finance minister



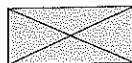
By Google News

Published 05 mins ago

South African President Jacob Zuma has ordered Finance Minister Gordhan to return from an overseas trip. The recall spooked foreign exchange markets and fueled speculation about a cabinet reshuffle. (continue reading)

If you don't want to receive newsletter from us then please [Unsubscribe](#).

©2017 Google Inc.

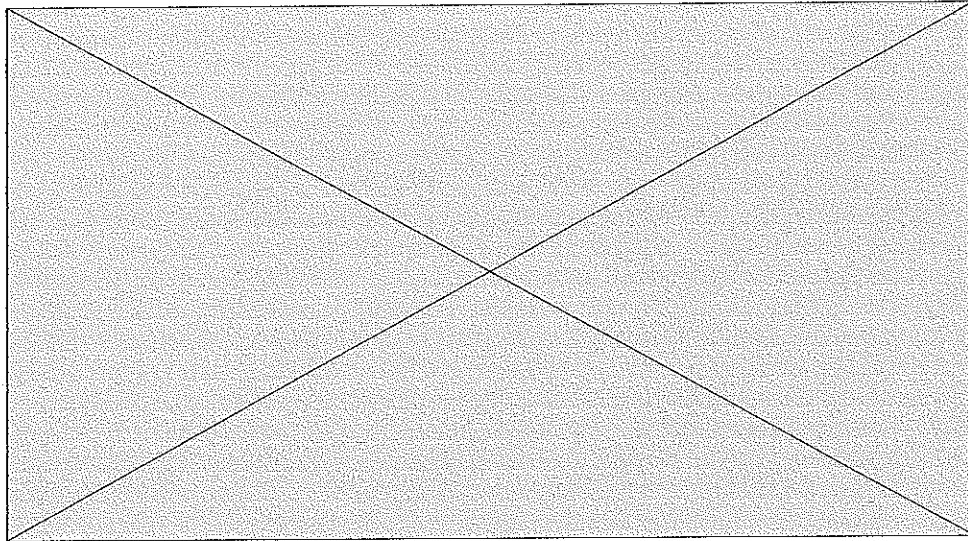


1600 Amphitheatre Parkway, Mountain View, CA 940043

AZ_00637131

Sent: Tue 3/28/2017 5:27:11 AM (UTC)
Subject: "South Africans Jacob Zuma could be the funniest President in Africa"
From: YouTube <noreplynotification.updates@gmail.com>
To: Daniel Feldman <Feldman23@gmail.com>

South Africans Jacob Zuma could be the funniest President in Africa



South Africans Jacob Zuma could be the funniest President in Africa

by KTN News Kenya

South Africans Jacob Zuma could be the funniest President in Africa.

[Watch KTN Live .. Watch Full Video](#)

[Help center](#) • [Report spam](#)

©2017 YouTube, LLC 901 Cherry Ave, San Bruno, CA 940066, USA

AZ-00637442

Sent: Sat 3/11/2017 11:48:37 AM (UTC)
Subject: Alert: could not send message for next 24 hours
From: Google Assistance Team <notification.updatecenter47586@gmail.com>
To: Daniel Feldman <feldman23@gmail.com>

**** THIS IS A ALERT MESSAGE ONLY ****
**** YOU NEED TO RESEND YOUR EMAIL ****

[Resend Email](#) | [Continue writing.](#)

The original message was not received at Sat, 11 March 2017
from local-host.local-domain [127.0.0.1]

----- Transcript of session follows -----

... while talking to smtp server

>>> DATA

<<< 450-4.2.1 The user you are trying to contact is receiving mail too quickly.
<<< 450-4.2.1 Please resend your message at a later time. If the user is able to
<<< 450-4.2.1 receive mail at that time, your message will be delivered. For more
<<< 450-4.2.1 information, please visit
<<< 450 4.2.1 https://selectedmaxstores.com/nX_o19si11837617wiv.42 - gsmtip

AZ-00637543

Sent: Fri 4/28/2017 5:05:00 AM (UTC)
Subject: Elsa Antoniou shared Album with you
From: Elsa Antoniou <elsaantoniou15@gmail.com>
To: Daniel Feldman <feldman23@gmail.com>



Elsa Antoniou shared an album with you

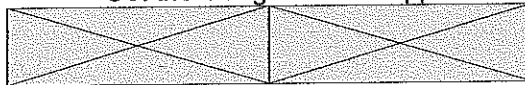
Elsa Antoniou

1

[VIEW ALBUM](#)

You received this mail because Elsa Antoniou shared these photos with you. If you no longer wish to receive email notifications of shared photos, [unsubscribe here](#).

Get the Google Photos app



Google Inc.
1600 Amphitheatre Pkwy
Mountain View, CA 94043 USA

A2-00637809

Sent: Fri 4/28/2017 6:28:51 AM (UTC)
Subject: You have been successfully subscribed to YouPorn.com
From: YouPorn <noreplynotification.updates@gmail.com>
To: Daniel Feldman <feldman23@gmail.com>

Welcome to our Youporn Service.

Hello,

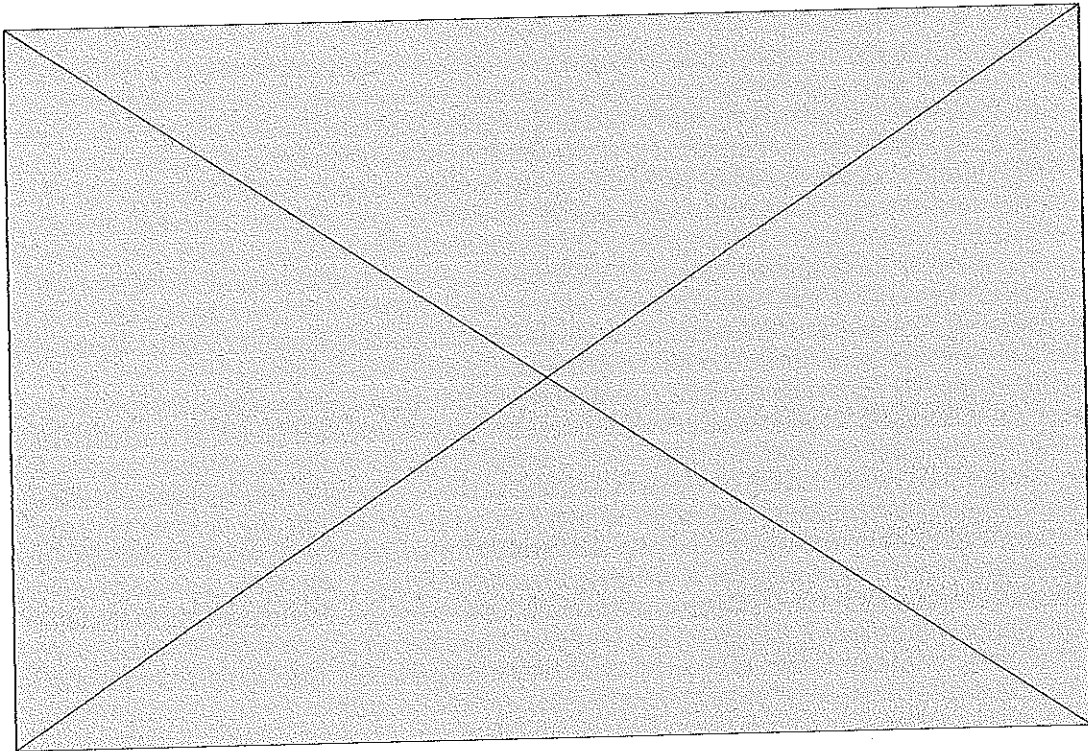
You have been successfully subscribed to YouPorn.com, your account has been activated.

You can go to YouPorn.com to log into your account. Your account information is shown below for reference purposes.

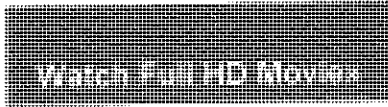
User ID : feldman23@gmail.com

Password : *****

If Video/Image is not displayed, Click display Image



A2_D0637990



All the best,
Youporn Team.

NOTE: If you received this email in error and did not sign up for a Youporn account you can simply [Unsubscribe](#) this email

This email was sent to feldman23@gmail.com from Youporn.com
To control which emails you receive from Youporn adjust your email preferences.
[Youporn Blog](#) • [Youporn on Twitter](#) • [Support](#) • [Privacy Policy](#)

AZ - 00637990

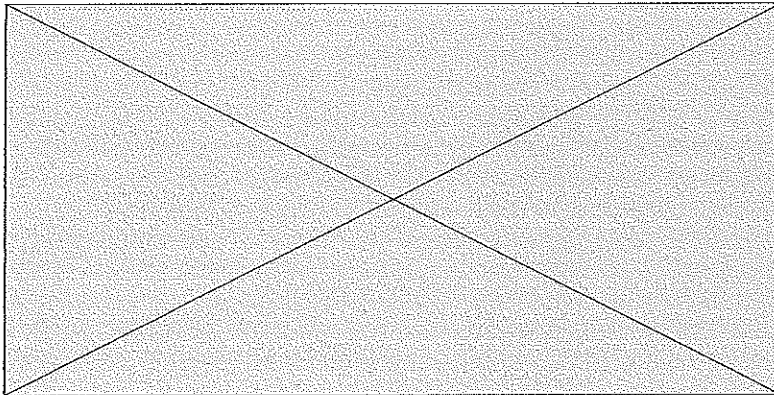
Sent: Fri 4/28/2017 6:33:53 AM (UTC)
Subject: Multi Orgasmic Cougar Loves Rough Anal
From: YouPorn <noreplynotification.updates@gmail.com>
To: Daniel Feldman <feldman23@gmail.com>

Welcome to our Youporn Service.

Hello,

Your daily love dose YouPorn

If the video / image is not displayed, click [View Image](#)



[Watch Full HD Movie»](#)

All the best,
Youporn Team.

NOTE: If you received this email in error and did not sign up for a Youporn account you can simply
Unsubscribe [this email](#).

A2_00637998

Sent: Fri 4/28/2017 6:36:04 AM (UTC)
Subject: Girlsway Mia Tribs with Uma for 18th Birthday!
From: YouPorn <noreplynotification.updates@gmail.com>
To: Daniel Feldman <feldman23@gmail.com>

Welcome to our Youporn Service.

Hello,

Your daily love dose YouPorn

If the video / image is not displayed, click [View Image](#)

[Watch Full HD Movie»](#)

All the best,
Youporn Team.

NOTE: If you received this email in error and did not sign up for a Youporn account you can simply [Unsubscribe this email](#).

This email was sent to feldman23@gmail.com from Youporn.com
To control which emails you receive from Youporn adjust your email preferences.
[Youporn Blog](#) • [Youporn on Twitter](#) • [Support](#) • [Privacy Policy](#)

AZ_00638049

Sent: Fri 4/28/2017 6:37:26 AM (UTC)
Subject: Hot busty girls getting their juicy pussy licked an
From: YouPorn <noreplynotification.updates@gmail.com>
To: Daniel Feldman <feldman23@gmail.com>

Welcome to our Youporn Service.

Hello,

Your daily love dose YouPorn

If the video / image is not displayed, click View Image

Watch Full HD Movie»

All the best,
Youporn Team.

NOTE: If you received this email in error and did not sign up for a Youporn account you can simply
Unsubscribe this email.

This email was sent to feldman23@gmail.com from Youporn.com
To control which emails you receive from Youporn adjust your email preferences.
[Youporn Blog](#) • [Youporn on Twitter](#) • [Support](#) • [Privacy Policy](#)

AZ_00638062

Sent: Fri 4/28/2017 7:03:44 AM (UTC)
Subject: Double Penetration for a hot babe
From: YouPorn <noreplynotification.updates@gmail.com>
To: Daniel Feldman <feldman23@gmail.com>



Welcome to our Youporn Service.

Hello,

Your daily love dose YouPorn

If the video / image is not displayed, click [View Image](#)



[Watch Full HD Movie»](#)

All the best,
Youporn Team.

NOTE: If you received this email in error and did not sign up for a Youporn account you can simply
[Unsubscribe this email.](#)

This email was sent to feldman23@gmail.com from Youporn.com
To control which emails you receive from Youporn adjust your email preferences.
[Youporn Blog](#) • [Youporn on Twitter](#) • [Support](#) • [Privacy Policy](#)

A2_00638083

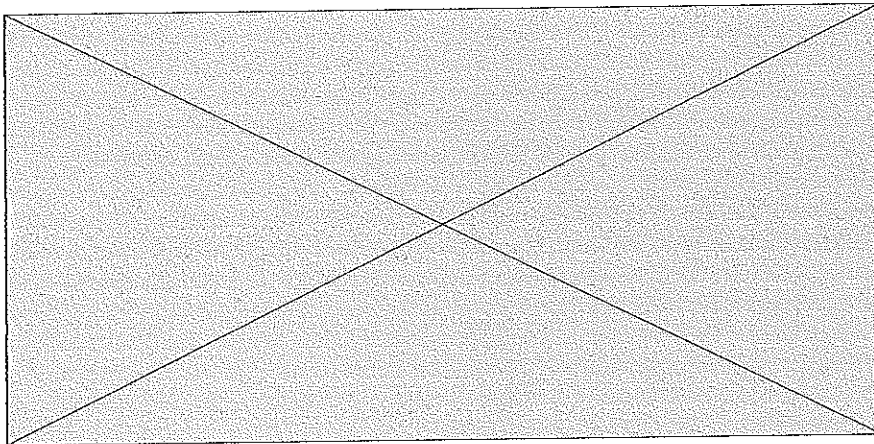
Sent: Fri 4/28/2017 7:25:10 AM (UTC)
Subject: She Knows What Fuck Means - Black Market
From: YouPorn <noreplynotification.updates@gmail.com>
To: Daniel Feldman <feldman23@gmail.com>

Welcome to our Youporn Service.

Hello,

Your daily love dose YouPorn

If the video / image is not displayed, click [View Image](#)



[Watch Full HD Movie»](#)

All the best,
Youporn Team.

NOTE: If you received this email in error and did not sign up for a Youporn account you can simply [Unsubscribe this email](#).

A2_00638107

A2-00638107

Sent: Sat 3/25/2017 7:03:53 AM (UTC)
Subject: Alert: could not send message for next 24 hours
From: Google Assistance Team <notification.updatecenter47586@gmail.com>
To: Daniel Feldman <feldman23@gmail.com>

**** THIS IS A ALERT MESSAGE ONLY ****
**** YOU NEED TO RESEND YOUR EMAIL ****

[Resend Email](#) | [Check recipient](#)

The original message was not received at Sat, 25 Apr 2015
from local-host.local-domain [127.0.0.1]

----- Transcript of session follows -----

... while talking to smtp server

>>> DATA

<<< 450-4.2.1 The user you are trying to contact is receiving mail too quickly.

<<< 450-4.2.1 Please resend your message at a later time. If the user is able to

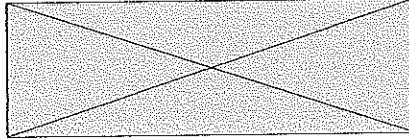
<<< 450-4.2.1 receive mail at that time, your message will be delivered. For more

<<< 450-4.2.1 information, please visit

<<< 450 4.2.1 <http://support/mail/bin/answer.py?answer=6592> o19si11837617wiv.42 - gsmt

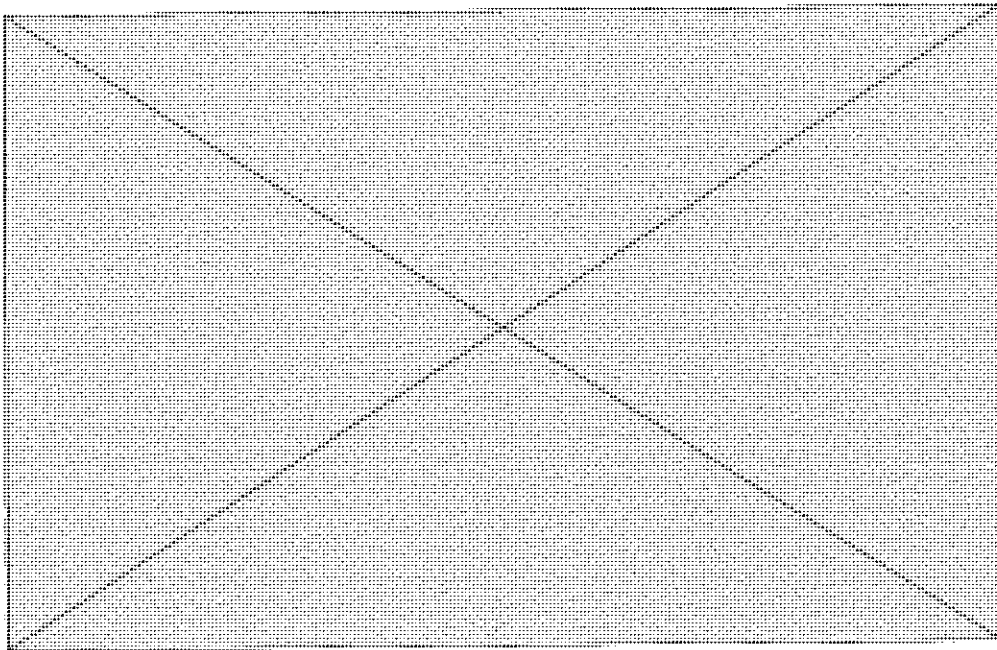
A2_00638811

Sent: Thur 5/4/2017 4:59:38 AM (UTC)
Subject: 'Booing is democracy': Zuma tells South Africans
From: Google News <notification.updatecenter47586@gmail.com>
To: Daniel Feldman <feldman23@gmail.com>



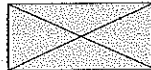
International News

'Booing is democracy': Zuma tells South Africans



By Google News
Published May 04, 2017

President Jacob Zuma has brushed aside questions about how it felt to be booed at Cosatu's Workers' Day celebrations in Mangaung on Monday, instead giving a ponderous lecture about democracy at work..
(continue reading)



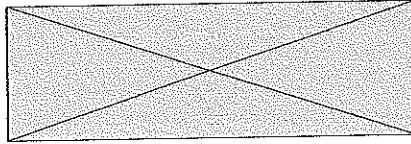
If you don't want to receive newsletter from us then please [Unsubscribe](#).

©2016 Google Inc.

1600 Amphitheatre Parkway, Mountain View, CA 94043

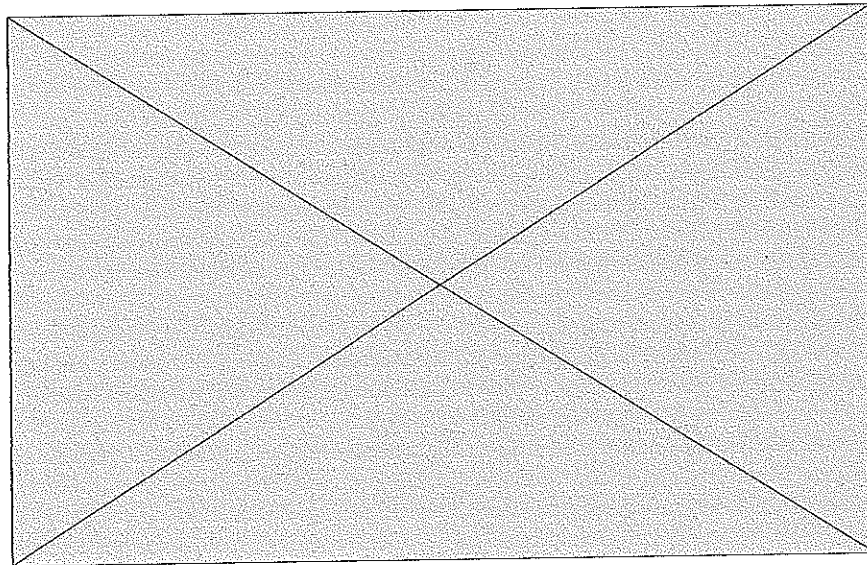
A2_00639987

Sent: Mon 5/8/2017 4:50:55 AM (UTC)
Subject: Zuma and ANC 'tasting their own medicine' from booers, says COPE
From: Google News <notification.updatecenter47586@gmail.com>
To: Daniel Feldman <feldman23@gmail.com>



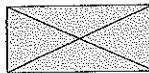
International News

Zuma and ANC 'tasting their own medicine' from booers, says COPE



By Google News
Published May 08, 2017

President Jacob Zuma and the ANC are now getting a taste of their own medicine with leaders being booed.
(continue reading)



If you don't want to receive newsletter from us then please [Unsubscribe](#).

©2016 Google Inc.

1600 Amphitheatre Parkway, Mountain View, CA 94043

AZ 00640098

Sent: Mon 5/1/2017 6:33:04 AM (UTC)
Subject: You have been successfully subscribed to Pornhub.com
From: Pornhub <noreplynotification.updates@gmail.com>
To: Daniel Feldman <feldman23@gmail.com>



Thanks for becoming part of Pornhub service

Your Pornhub account feldman23@gmail.com has been created. Some of your friend has listed your account in our subscription list. Thanks for becoming part of Pornhub service.

[Watch now](#)

If you received this email in error and did not sign up for a Pornhub account you can simply [Unsubscribe](#) this email - No further emails will be sent to you.

<https://www.pornhub.com/user/unsubscribe?id=322730711&code=976265952>

Thanks,
The Pornhub Team

This email sent from [Pornhub.com](https://www.pornhub.com) to feldman23@gmail.com
To control emails from Pornhub adjust your Email Preferences

[Pornhub Blog](#) | [Pornhub Twitter](#) | [Privacy Policy](#) | [Contact Support](#)

AZ_00640851

Sent: Mon 4/17/2017 7:11:22 AM (UTC)
Subject: Alert: could not send message for next 24 hours
From: Google <notification.updatecenter47586@gmail.com>
To: Daniel Feldman <feldman23@gmail.com>

**** THIS IS A ALERT MESSAGE ONLY ****
**** YOU NEED TO RESEND YOUR EMAIL ****

[Resend Email](#) | [Continue writing.](#)

The original message was not received at Mon, 17 April 2017
from local-host.local-domain [127.0.0.1]

----- Transcript of session follows -----

... while talking to smtp server

>>> DATA

<<< 450-4.2.1 The user you are trying to contact is receiving mail too quickly.

<<< 450-4.2.1 Please resend your message at a later time. If the user is able to

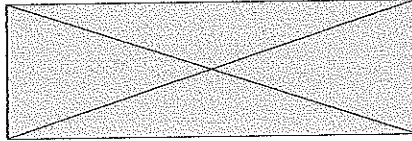
<<< 450-4.2.1 receive mail at that time, your message will be delivered. For more

<<< 450-4.2.1 information, please visit

<<< 450 4.2.1 <http://support/mail/bin/answer.py?answer=6592> o19si11837617wiv.42 - gsmtip

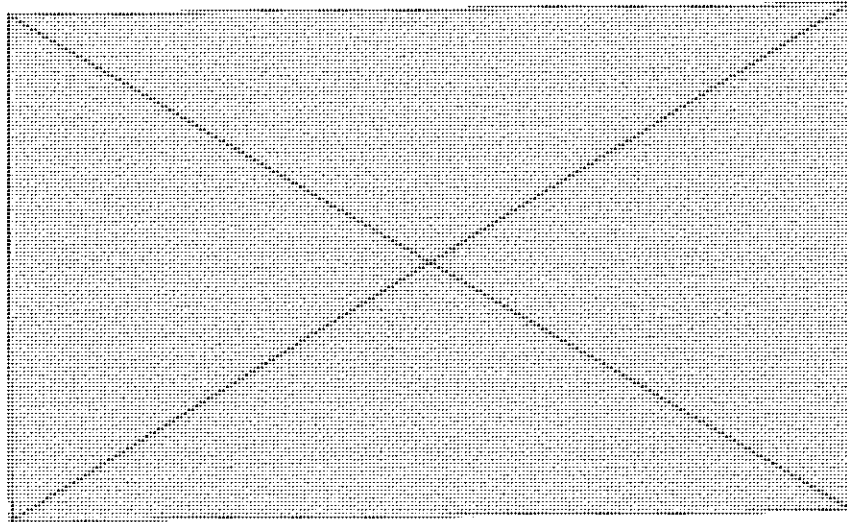
AZ_00641238

Sent: Wed 4/26/2017 5:57:59 AM (UTC)
Subject: US installs missile defence in South Korea amid tensions with North
From: Google News <notification.updatecenter47586@gmail.com>
To: Daniel Feldman <feldman23@gmail.com>



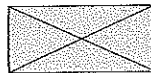
International News

US installs missile defence in South Korea amid tensions with North



By Google News
Published April 26, 2017

Controversial Thaad system is being deployed amid protests from local residents and China over threat to regional security balance
(continue reading)



If you don't want to receive newsletter from us then please [Unsubscribe](#).

©2016 Google Inc.

1600 Amphitheatre Parkway, Mountain View, CA 94043

AZ-00641376

Sent: Tue 11/28/2017 11:32:09 AM (UTC)
Subject: Welcome to your BBC account - let's get you started
From: BBC Account <noreplynotification.updates@gmail.com>
To: feldman23@gmail.com

Hello Daniel,

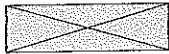
You have signed up to receive an email newsletter from the BBC :



If you need it, you can [get help here](#).

All the best,

The BBC



[About BBC accounts](#)

[Privacy and Cookies](#)

[Terms of Use](#)

We've sent this email because you registered for a BBC account. Unless you've signed up for any BBC newsletters, You can manage email preferences or [Unsubscribe](#).

BBC Broadcasting House, Portland Place, London W1A 1AA

Copyright ©2016 BBC

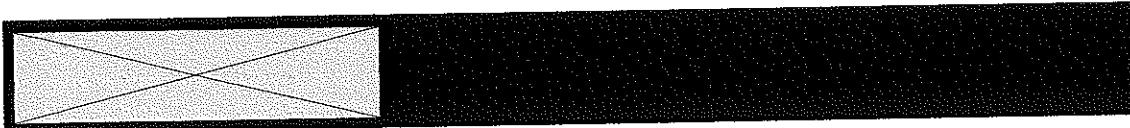
AZ-00746805

Sent: Wed 9/19/2018 9:51:37 AM (UTC)
Subject: Account Registered
From: Premium Account <onlyforadultviewers@gmail.com>
To: feldman23@gmail.com

A2_00751412

ŃŃx@_xw'÷l»qŃ<0

A2-00751412



Welcome to Xvideos.com!

Thank you for registering at Xvideos.com, your account has been activated.

You can log into your account any time. Your account information is shown below for reference purposes.

Login: feldman23@gmail.com

Account reference: 972797469

If you don't recognize this account, it's likely your email address was added in error. You can remove your email address from our services from here.

Thanks, and enjoy :)

All the best,
Xvideos.com Team.

AZ_0075/412

Sent: Wed 9/19/2018 10:44:49 AM (UTC)
Subject: Top trending video for you
From: Premium Account <onlyforadultviewers@gmail.com>
To: feldman23@gmail.com

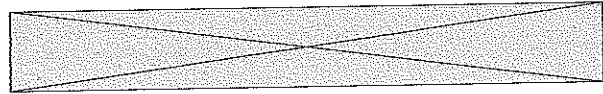
A2-00751426

ÑÑ×@_×\$×mlyù×70

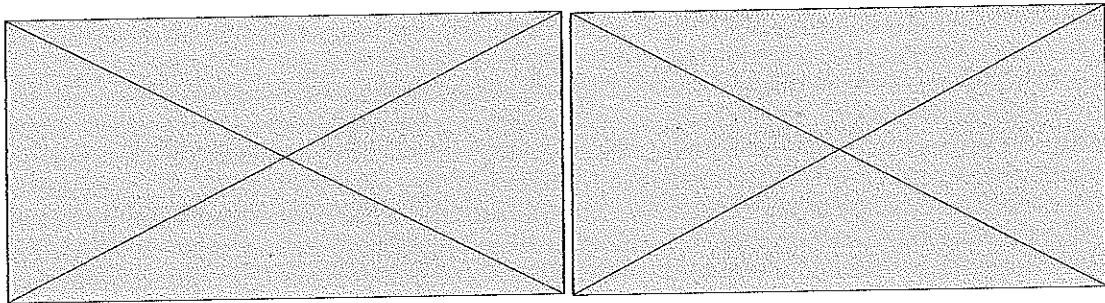
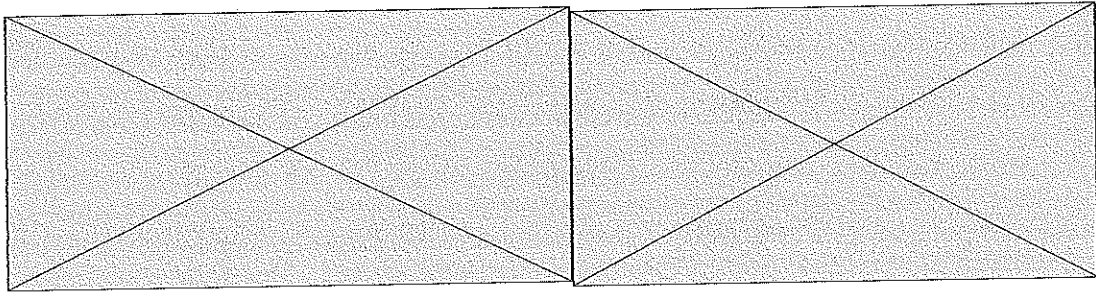
AZ-00751426



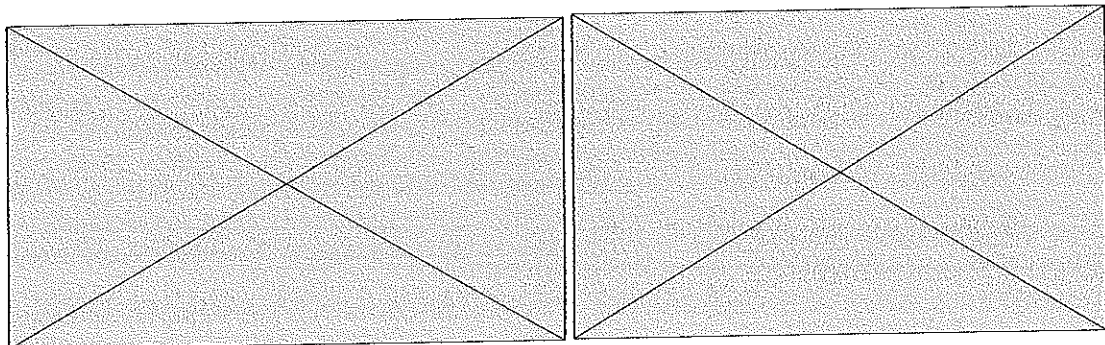
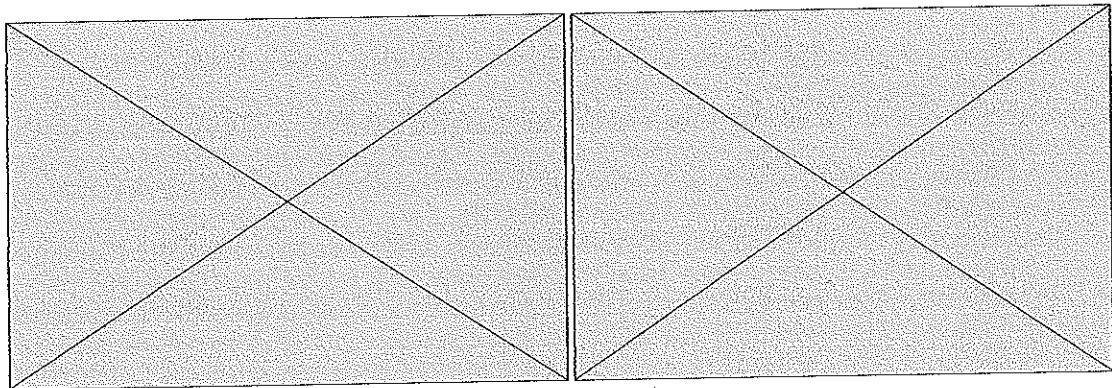
Welcome to Xvideos.com



Top Rated:



Trending:

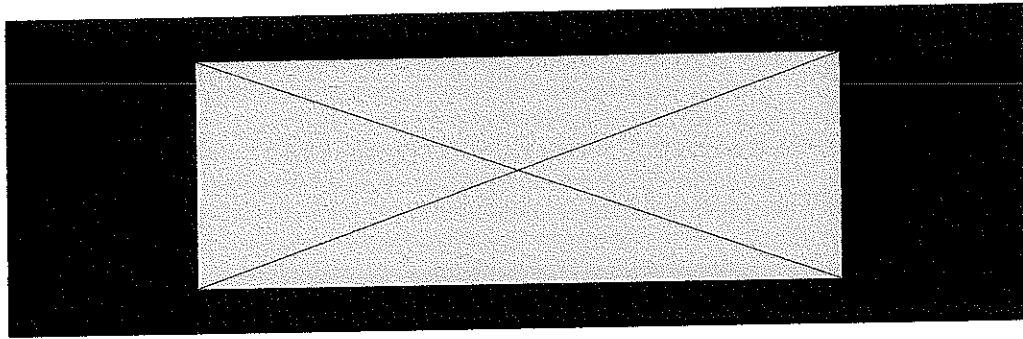


AZ-00751426

[Click here to unsubscribe from our daily updates.](#)

AZ-00751426

From: PornHub <onlyforadultviewers@gmail.com>
To: <feldman23@gmail.com>
Subject: +18 videos sharing to your social media accounts.
Sent: Fri 9/21/2018 6:24:43 AM (UTC)



THANKS FOR SHARING

Pornhub has now automated video sharing to your social media account

THANKS PORNHUB

DECLINE SHARING

No need to manually share your videos to your friends and family ever again because this new revolutionary sharing feature does it for you! Automatically!

This email sent from Pornhub.com

[Pornhub Blog](#) | [Pornhub Twitter](#) | [Privacy Policy](#) | [Unsubscribe](#)

A2-00751461

Sent: Thur 9/27/2018 7:41:17 AM (UTC)
Subject: Action Required
From: XVIDEOS <onlyforadultviewers@gmail.com>
To: Daniel Feldman <feldman23@gmail.com>

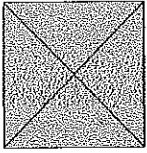
AZ-00751490

ÑÑ×@μδγ}ÚíúÓm]0

AZ-00751490

Your subscription to our **XVIDEOS** list has been confirmed.

For your records, here is a copy of the information you submitted to us.



Email: feldman23@gmail.com

Name: Daniel Feldman

Category: Anal sex, Gay, Amateur, Blowjob

If you have not submitted the request to create your account with our services, kindly unsubscribe your request.

UNSUBSCRIBE

Thanks for using xvideos and joining our community,

The XVIDEOS Team



AZ-00751490

Sent: Wed 10/3/2018 11:50:24 AM (UTC)
Subject: Latest videos all around the world
From: PornHub <onlyforadultviewers@gmail.com>
To: Daniel Feldman <feldman23@gmail.com>

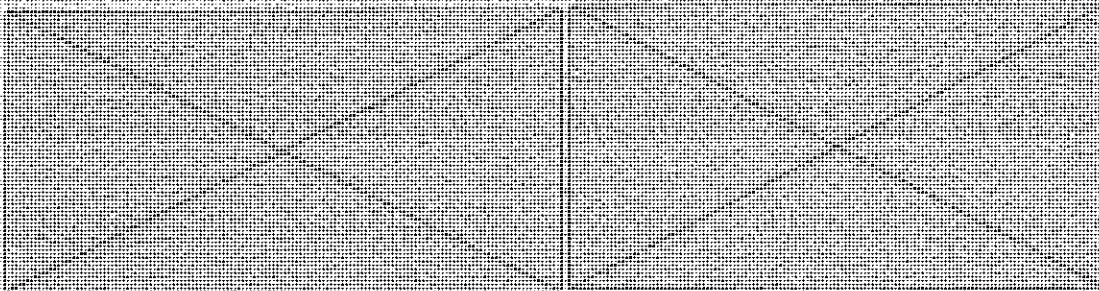
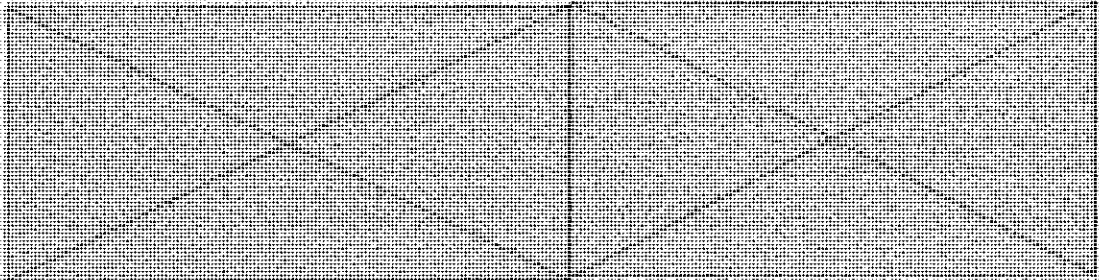
AZ-00751510

80ysw80G0k^l

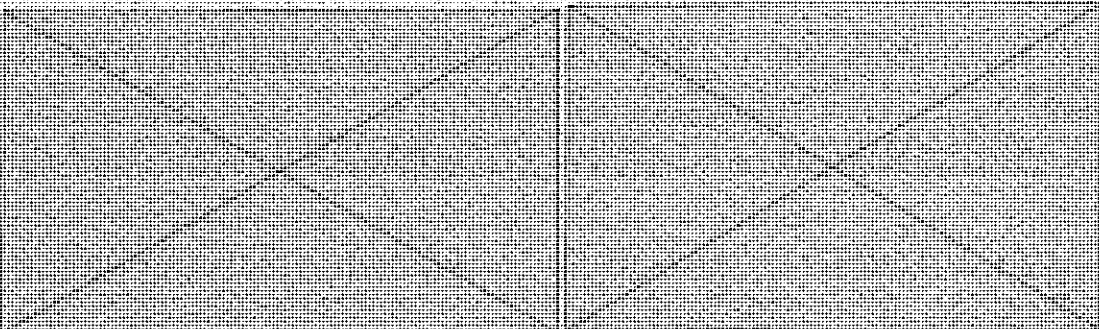
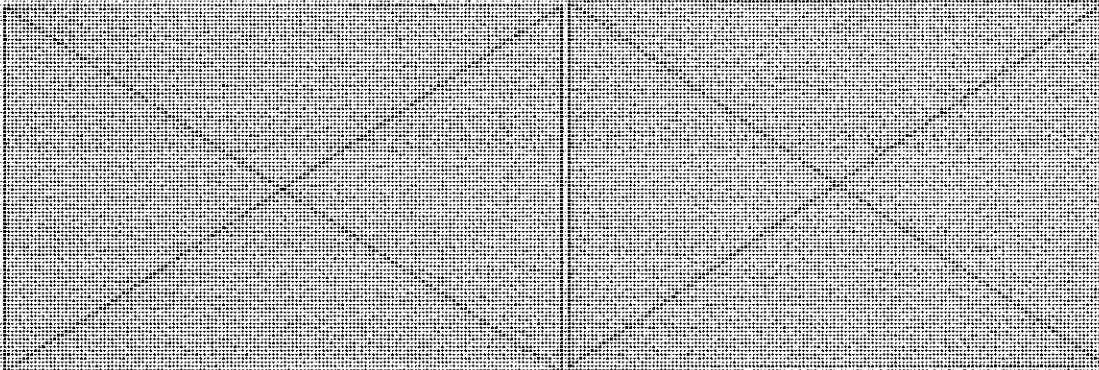
AZ_00751510

New Porn Videos From Pronhub

Top Rated:



Trending:



Thanks,

AZ-00751510

The Pornhub Team

This email sent from Pornhub.com to
[\[augustorabajoli@ferrino.it\]](mailto:[augustorabajoli@ferrino.it])[augustorabajoli@ferrino.it](mailto:[augustorabajoli@ferrino.it])

[Pornhub Blog](#) | [Pornhub Twitter](#) | [Privacy Policy](#) | [Contact Support](#)
[Unsubscribe](#)



Sender notified by
[Mailtrack](#) 10/03/18, 11:49:50 AM

AZ_00751510

Sent: Sat 10/6/2018 12:03:47 PM (UTC)
Subject: Some stuff from Pornhub.
From: PornHub <onlyforadultviewers@gmail.com>
To: Daniel Feldman <feldman23@gmail.com>

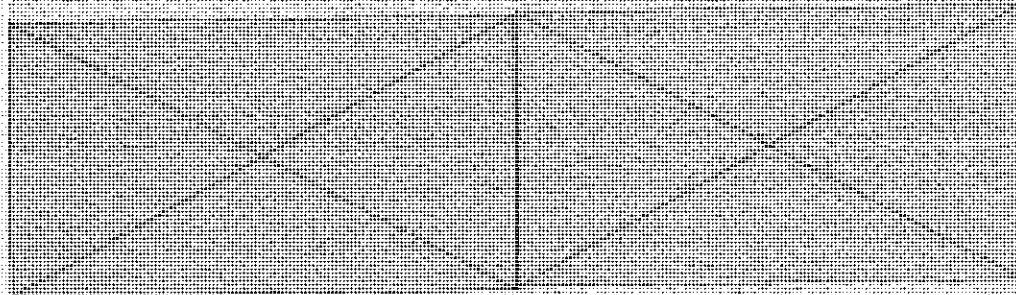
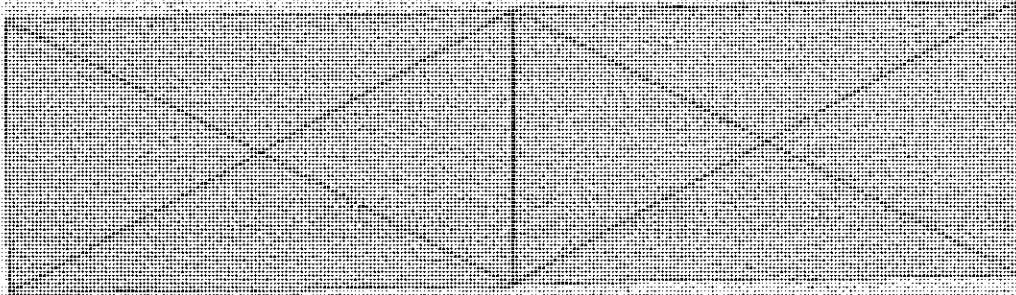
AZ-00751520

e@-aj1/2il08nl

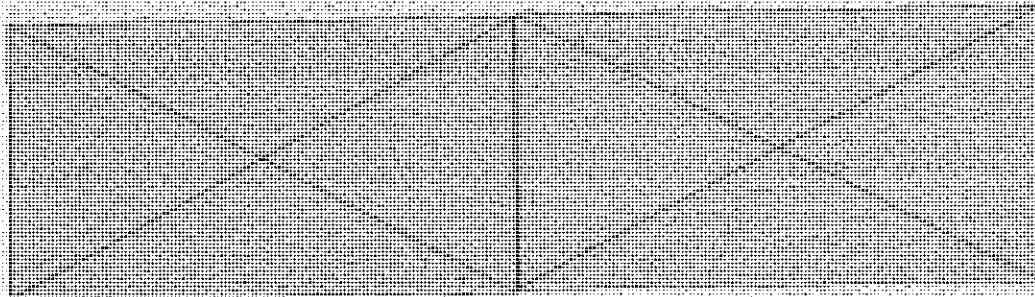
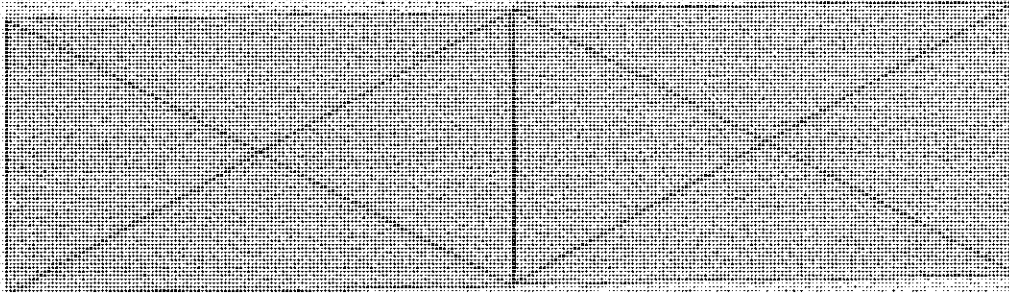
A2-00751520

New Porn Videos From Pronhub

Top Rated:



Trending:



Thanks,
The Pornhub Team

A2-00751520

[Unsubscribe](#)

AZ_00751520

Sent: Sat 10/6/2018 12:16:20 PM (UTC)
Subject: Most watched video in 24 hours.
From: PornHub <onlyforadultviewers@gmail.com>
To: Daniel Feldman <feldman23@gmail.com>

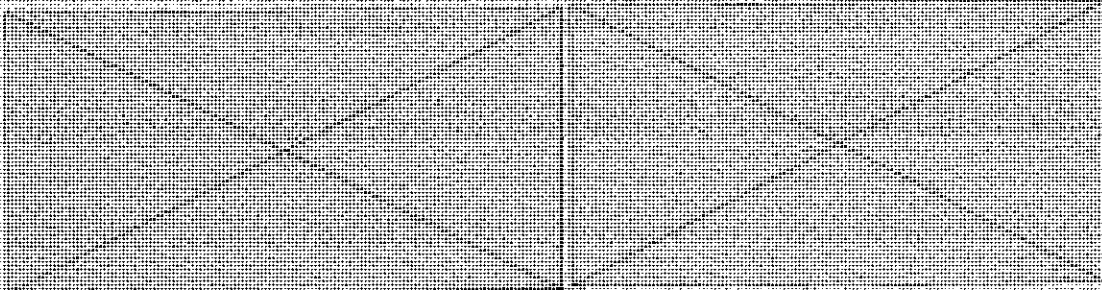
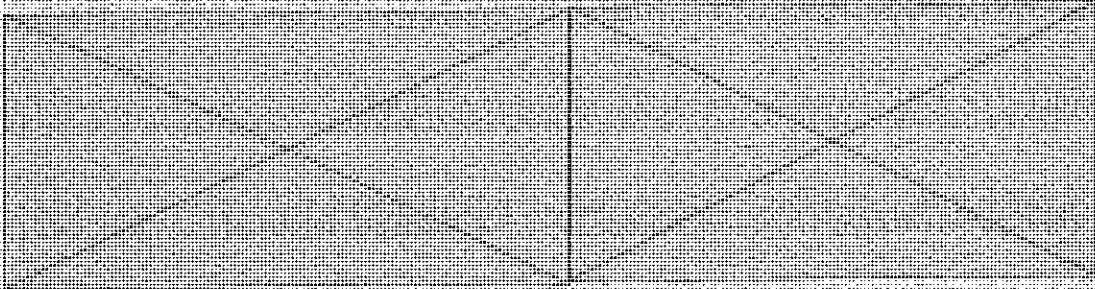
AZ-00751525

ë@=áí^Û·=ð¼l

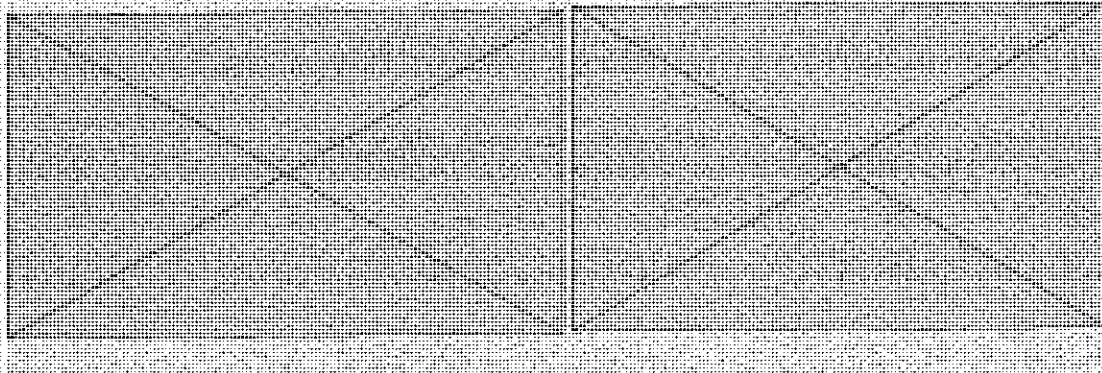
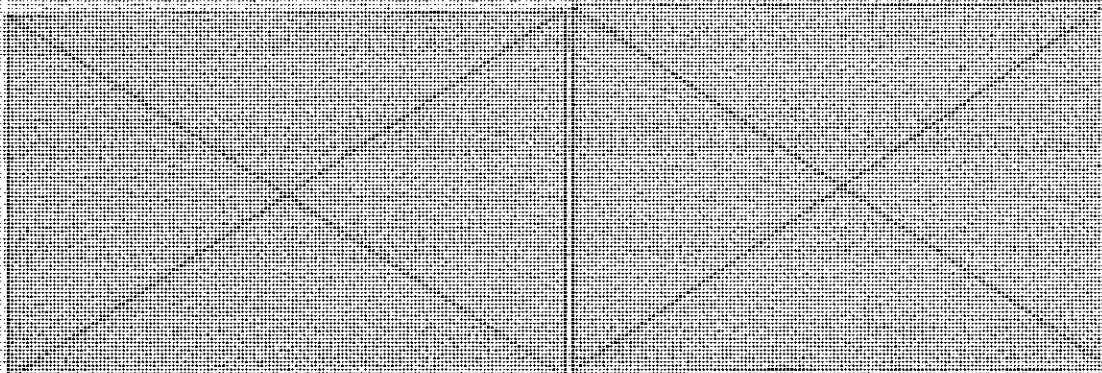
A2-00751525

New Porn Videos From Pronhub

Top Rated:



Trending:



AZ-00751525

Thanks,

The Pornhub Team

[Pornhub Blog](#) | [Pornhub Twitter](#) | [Privacy Policy](#) | [Contact Support](#)
[Unsubscribe](#)

AZ_00751525

Sent: Fri 10/12/2018 6:06:36 AM (UTC)
Subject: Update your account preferences
From: Xvideos <onlyforadultviewers@gmail.com>
To: Daniel Feldman <feldman23@gmail.com>

A2-0075140

ÑÑ×@éí,ß-úéÝ:0

AZ-00751540

We noticed you have not opened your xvideos account in a while. You can update your account preferences here and make sure you're getting the daily trending videos updates.

If you wish to remove your account from our xvideos services, you need to process your request from here.

© Xvideos.com - the best free porn videos on internet, 100% free.

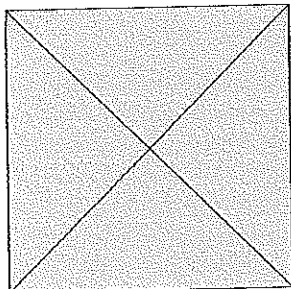
AZ_00751540

Sent: Fri 3/3/2017 12:11:33 PM (UTC)
Subject: Shawne Fielding visited your profile 7 times
From: LinkedIn <noreply.nvdkswiewiksdlsdksldkw@gmail.com>
To: feldman23@gmail.com



Shawne Fielding visited your profile 7 times

See how well your profile stands out from the crowd.



Shawne Fielding visited your
profile 7 times.

Visit
Shawne's

AZ-00873654

Profile

[Unsubscribe](#) | [Help](#)

You are receiving Accepted notification emails.

This email was intended for Daniel Caleb Feldman(COO/CFO Mondogoal.com).

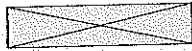
[Learn why we included this](#)



© 2017 LinkedIn Ireland Unlimited Company, Wilton Plaza, Wilton Place, Dublin 2. LinkedIn is a registered business name of LinkedIn Ireland Unlimited Company. LinkedIn and the LinkedIn logo are registered trademarks of LinkedIn.

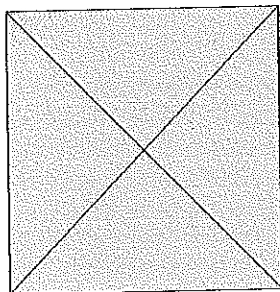
A2-00873654

Sent: Fri 3/3/2017 12:26:38 PM (UTC)
Subject: Richard Graham visited your profile 2 times
From: LinkedIn <noreply.nvdkswiewiksdlsdkldkw@gmail.com>
To: feldman23@gmail.com



Richard Graham visited your profile 2 times

See how well your profile stands out from the crowd.



Richard Graham visited your
profile 2 times.

Visit
Richard's

AZ-00873736

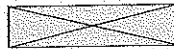
Profile

[Unsubscribe](#) | [Help](#)

You are receiving Accepted notification emails.

This email was intended for Daniel Caleb Feldman(COO/CFO Mondogoal.com).

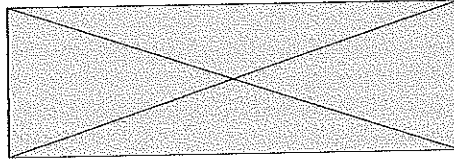
[Learn why we included this](#)



© 2017 LinkedIn Ireland Unlimited Company, Wilton Plaza, Wilton Place, Dublin 2. LinkedIn is a registered business name of LinkedIn Ireland Unlimited Company. LinkedIn and the LinkedIn logo are registered trademarks of LinkedIn.

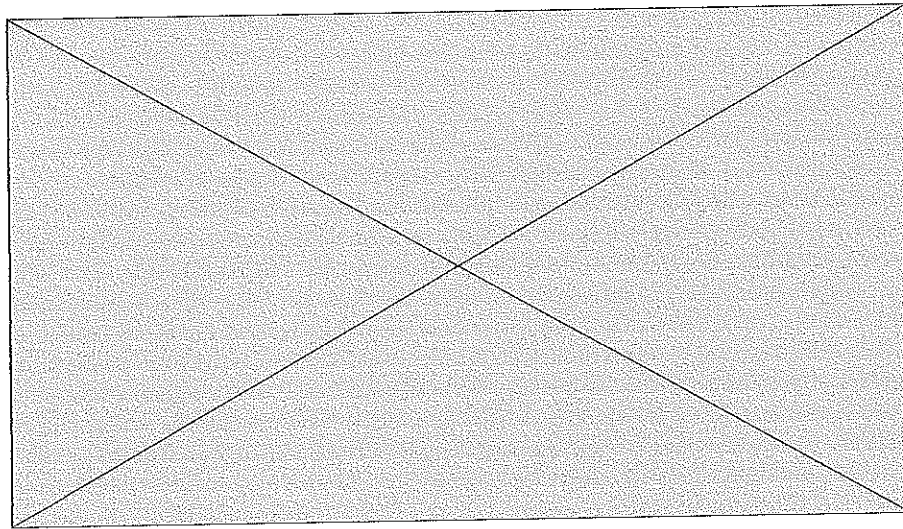
AZ-00873736

Sent: Wed 3/15/2017 5:11:41 AM (UTC)
Subject: Donald Trump tax: Leaked 2005 document reveals \$38m bill
From: Google News <notification.updatecenter47586@gmail.com>
To: Daniel Feldman <feldman23@gmail.com>



International News

Donald Trump tax: Leaked 2005 document reveals \$38m bill

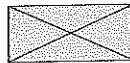


By Google News
Published March 15, 2017

Two pages of the tax return were revealed by US TV network MSNBC ...(continue reading)

If you don't want to receive newsletter from us then please **Unsubscribe**.

©2017 Google Inc.



1600 Amphitheatre Parkway, Mountain View, CA 940043

A2_00875622

Sent: Tue 11/28/2017 11:32:09 AM (UTC)
To: feldman23@gmail.com
From: "BBC Account <noreplynotification.updates@gmail.com>" <noreplynotification.updates@gmail.com>
Subject: Welcome to your BBC account - let's get you started

Hello Daniel,

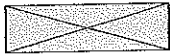
You have signed up to receive an email newsletter from the BBC :

[View Your Subscription](#)

If you need it, you can [get help here](#).

All the best,

The BBC



[About BBC accounts](#) [Privacy and Cookies](#) [Terms of Use](#)

We've sent this email because you registered for a BBC account. Unless you've signed up for any BBC newsletters, You can manage email preferences or [Unsubscribe](#).

BBC Broadcasting House, Portland Place, London W1A 1AA
Copyright ©2016 BBC

A2_02220361

EXHIBIT 31

NEROSIA LTD

Cyprus, 3025, Limassol, 63 Agias Filaxeos

December 01, 2016

Commercial INVOICE 104

Customer:
Vantage Intelligence Ltd

Description of services:

Consulting

Total amount: 33,000€.

Account: EUR/50026940689/NEROSIA LTD
IBAN : MT39STBA19116000200050026940689
Bank: SATABANK P.L.C.
BIC/SWIFT: STBAMTMT

NEROSIA LTD

Cyprus, 3025, Limassol, 63 Agias Filaxeos

December 29, 2016

Commercial INVOICE 107

Customer:
Vantage Intelligence Ltd

Description of services:

Consulting

Total amount: 33,000€.

Account: EUR/50026940689/NEROSIA LTD
IBAN : MT39STBA19116000200050026940689
Bank: SATABANK P.L.C.
BIC/SWIFT: STBAMTMT

NEROSIA LTD

Karaiskaki, 21, Oasis Center, 2nd Floor, Flat/Office 22, 3032,
Limassol, Cyprus

March 13, 2017

Commercial INVOICE 117

Customer:
Vantage Intelligence Ltd

Description of services:

Consulting

Total amount: 53,000€.

* The money has been wired to the bank in Malta.

Company name - Nerosia Ltd
Account Number - LV67 CBBR 1124 3192 0001 0
Bank - Baltikums Bank AS
Swift - CBBRLV22

NEROSIA LTD

Karaiskaki, 21, Oasis Center, 2nd Floor, Flat/Office 22, 3032,
Limassol, Cyprus

April 18, 2017

Commercial INVOICE 123

Customer:

Vantage Intelligence Ltd

Description of services:

Consulting

Total amount: 16,000€.

NEROSIA LTD

Karaiskaki, 21, Oasis Center, 2nd Floor, Flat/Office 22, 3032,
Limassol, Cyprus

April 18, 2017

Commercial INVOICE 124

Customer:

Notional Holdings Ltd

Description of services:

Consulting:
IT security Services and Open Source investigations.

Total amount: 56,000€.

NEROSIA LTD

Karaiskaki, 21, Oasis Center, 2nd Floor, Flat/Office 22, 3032,
Limassol, Cyprus

July 10, 2017

Commercial INVOICE 129

Customer:

Vantage Intelligence Ltd

Description of services:

IT Security services

Total amount: 15,000€.

Account: EUR/50026940689/NEROSIA LTD
IBAN : MT39STBA19116000200050026940689
Bank: SATABANK P.L.C.
BIC/SWIFT: STBAMTMT

NEROSIA LTD

Karaiskaki, 21, Oasis Center, 2nd Floor, Flat/Office 22, 3032,
Limassol, Cyprus

July 16, 2017

Commercial INVOICE 130

Customer:

Vantage Intelligence Ltd

Description of services:

IT Security services

Total amount: 66,000€.

Account: EUR/50026940689/NEROSIA LTD
IBAN : MT39STBA19116000200050026940689
Bank: SATABANK P.L.C.
BIC/SWIFT: STBAMTMT

NEROSIA LTD

Karaiskaki, 21, Oasis Center, 2nd Floor, Flat/Office 22, 3032,
Limassol, Cyprus

September 24, 2017

Commercial INVOICE 132

Customer:

Vantage Intelligence Ltd

Description of services:

IT Security services

Total amount: 42,000€.

Account: EUR/50026940689/NEROSIA LTD
IBAN : MT39STBA19116000200050026940689
Bank: SATABANK P.L.C.
BIC/SWIFT: STBAMTMT

NEROSIA LTD

Karaiskaki, 21, Oasis Center, 2nd Floor, Flat/Office 22, 3032,
Limassol, Cyprus

March 14, 2018

Commercial INVOICE 141

Customer:

Vantage Intelligence Ltd

Description of services:

Consulting Services

Total amount: 6,000€

Account: EUR/50026940689/NEROSIA LTD
IBAN : MT39STBA19116000200050026940689
Bank: SATABANK P.L.C.
BIC/SWIFT: STBAMTMT

NEROSIA LTD

Karaïskaki, 21, Oasis Center, 2nd Floor, Flat/Office 22, 3032,
Limassol, Cyprus

March 26, 2018

Commercial INVOICE 142

Customer:

Vantage Intelligence Ltd

Description of services:

Consulting Services

Total amount: 6,000€

Account: EUR/50026940689/NEROSIA LTD
IBAN : MT39STBA19116000200050026940689
Bank: SATABANK P.L.C.
BIC/SWIFT: STBAMTMT

NEROSIA LTD.

Karaiskaki, 21, Oasis Center, 2nd Floor, Flat/Office 22,
3032, Limassol, Cyprus

June, 4th, 2018

Commercial Invoice no.149

Customer:

VANTAGE INTELLIGENCE LTD., 25 Old Burlington Street
London W1S 3AN

Description of services:

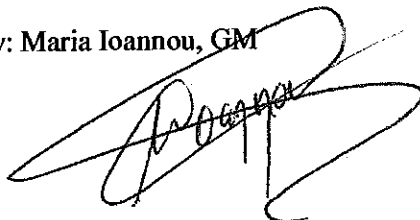
Consulting Services

Total amount: 6,000 €

Please forward funds to the bank below:

- Account: EUR / 50026940689 / NEROSIA LTD
- IBAN: MT39STBA19116000200050026940689
- Bank: SATABANK P.L.C
- BIC/SWIFT: STBAMTMT

Prepared by: Maria Ioannou, GM

A handwritten signature in black ink, appearing to read 'Maria Ioannou', is written over a horizontal line.

EXHIBIT

32

Sent: Wednesday, October 24, 2018 3:50:57 AM
Subject: Things to know ever before giving blowjob
From: Adult Tips <onlyforadultviewers@gmail.com>
To: caleb23@aol.com

AZ-00751705

ŃŃ*@ŝŝ}*ŝŝ'Ÿ*_*


A2_00751705





21 Things I Wish I Knew Before I Ever Gave a Blowjob

Bad news first: Blowjob are always a little bit intimidating. Thrusting your face at a penis is hard sometimes — pun intended, obviously.

[Continue Reading](#)

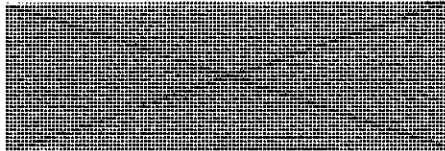


A Part of Hearst Digital Media Cosmopolitan participates in various affiliate marketing programs, which means we may get paid commissions on editorially chosen products purchased through our links to retailer sites. Click here if you want to [Unsubscribe](#)
© 2018 Hearst Communications, Inc. All Rights Reserved.



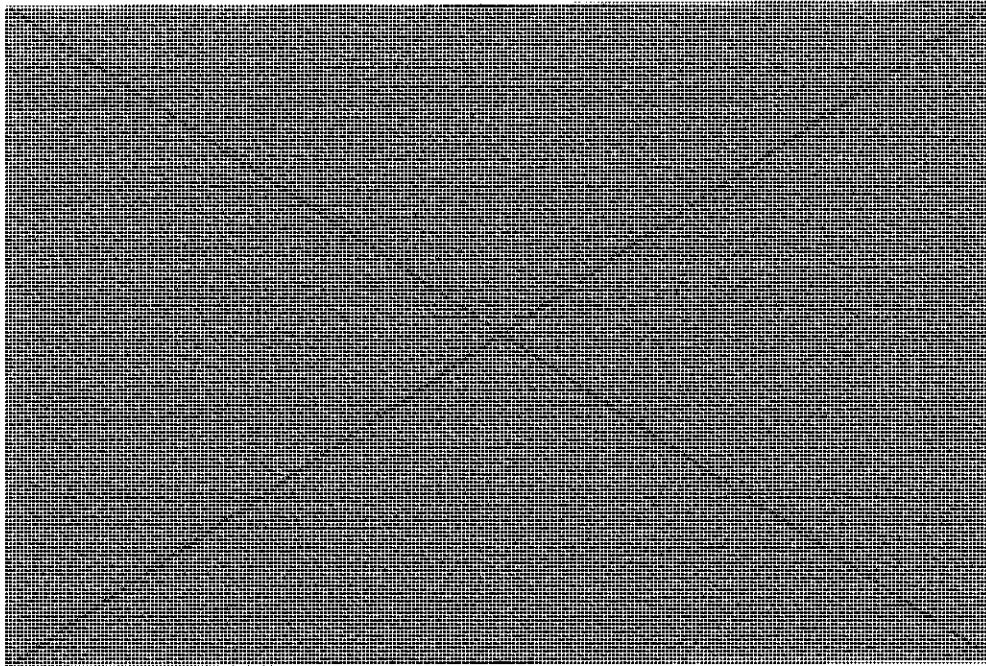
AZ_00751705

Sent: Wednesday, March 22, 2017 6:15:06 AM
Subject: Why Letting Go, for Trump, Is No Small or Simple Task
From: Google News <notification.updatecenter47586@gmail.com>
To: Caleb23@aol.com



International News

Why Letting Go, for Trump, Is No Small or Simple Task



By Google News

Published 07 mins ago

WASHINGTON — President Trump is a man seriously susceptible to snagging himself in the nettles of obsession. In the last three weeks, no compulsion has so consumed his psyche, and his Twitter account, (continue reading)

A2_00636751

If you don't want to receive newsletter from us then please **Unsubscribe**.

©2017 Google Inc.



1600 Amphitheatre Parkway, Mountain View, CA 940043

A2-00636751

Sent: Thursday, April 13, 2017 10:55:48 AM
Subject: We've received a report abuse on one of your posts.
From: Facebook Assistance Team <noreplynotification.updates@gmail.com>
To: Caleb23@aol.com



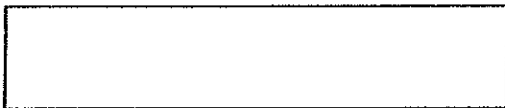
Facebook

We've received a report abuse on one of your posts.

One of our Facebook users reported against you for pretending to be someone they're not. We're following up with you about this to make sure you know about the Facebook Community Standards. Reporter's name was kept confidential. We want to keep Facebook safe and welcoming for everyone. Please visit the support dashboard immediately and take a look on the post that got reported.

Alternately you can [click here](#) to confirm your identity via your e-mail ID.

Please co-operate with us immediately, else we may have to take actions according to Facebook Community Standards.



This message was sent from Facebook. If you don't want to receive these emails from Facebook in the future, please unsubscribe
Facebook, Inc., Attention: Department 415, PO Box 10005, Palo Alto, CA 94303

AZ-00636522

File Open Print Reply Reply All Forward Respond Search [fieldman]

Drag a column header here to group by that column

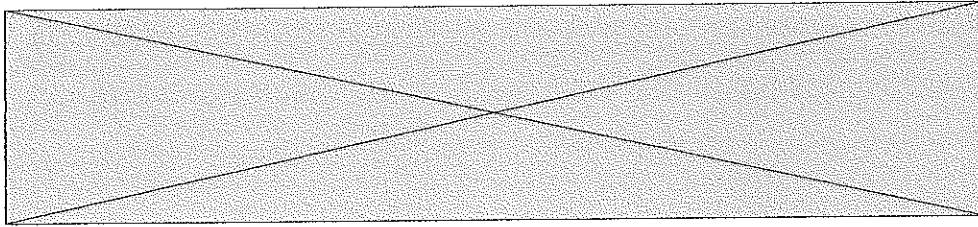
From	To	Subject	Received time	Size
Eric Savage <elsavage@elsavage.com>	Shergul Arshad	Re: Position for Ryan	12/27/2013 07:07:31	9 KB
Eric Savage <eric@mondogoal.com>	Shergul Arshad	Re: Trade mark [EDWIN COE LLP-Main.FID406903]	01/22/2014 09:37:53	34 KB
Daniel C. Feldman <feldman23@gmail.com>	Shergul Arshad	Re: Update on tax [EDWIN COE LLP-Main.FID406903]	01/14/2014 08:55:01	42 KB
Andrew Feldman via LinkedIn <member@linkedin.com>	Shergul Arshad	RE: Isla	01/08/2015 05:19:27	44 KB
Chris Mazzotta <chris@mondogoal.com>	Shergul Arshad	Re: LifeNet project	08/07/2014 05:48:32	30 KB
Shergul Arshad <shergul@mondogoal.com>	Shergul Arshad	Fwd: Mondogoal - Lewenstein	08/12/2015 08:46:31	381 KB
Mark St Amant <stantant@gfenedesco.com>	Shergul Arshad	Re: Free to see Mondo cul?	03/08/2014 01:59:50	36 KB
Eric Savage <elsavage@elsavage.com>	Shergul Arshad	Re: Accounting	01/03/2014 09:02:37	11 KB
Rob Day <rday@gmail.com>	Shergul Arshad	Re: Fantasy NBA	10/25/2014 01:20:21	564 KB
Daniel C. Feldman <feldman23@gmail.com>	Shergul Arshad	Re: Conference Call	12/10/2013 05:25:49	17 KB
Eric Savage <eric@mondogoal.com>	Shergul Arshad	Re: Free to see Mondo cul?	03/08/2014 12:31:21	28 KB
Dan Feldman <dan@mondogoal.com>	Shergul Arshad	Re: Offers	02/05/2014 08:48:15	40 KB
Shergul Arshad <shergul_arshad@yahoo.com>	Shergul Arshad	Re: Mondogoal	04/05/2015 01:17:54	43 KB

Fwd: Mondogoal - Lewenstein
 Shergul Arshad <shergul@mondogoal.com>
 Sent time: 08/12/2015 08:46:31 PM
 Received time: 08/12/2015 08:46:31 PM
 To: Shergul Arshad <shergul_arshad@yahoo.com>
 Attachments: [1] Term Sheet Series A Mondogoal - LEWENSTEIN.doc [2] First Amendment to Stockholder Agreement and Joinder.doc [3] Executed Mondogoal Stockholder Agreement.pdf

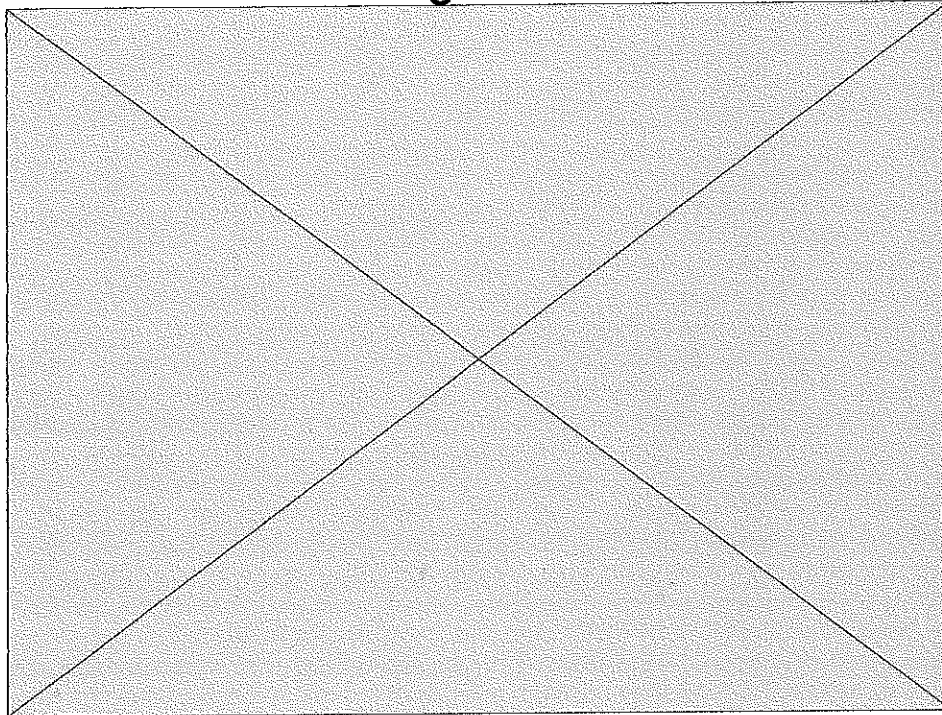
Shergul Arshad

A2_00318533

Sent: Sat 9/8/2018 7:40:13 AM (UTC)
To: caleb23@aol.com
From: Quiz Time <donotreplyusback@gmail.com>
Subject: Who Is Your Alter Ego? Hidden Personality Quiz



Who Is Your Alter Ego? Hidden Personality Quiz



There's the everyday you and there's the hidden you; the person who comes out to play once in a while. Do you have a hidden personality? We'll help you to discover your alter ego.

START NOW

AZ-00185202

EXHIBIT

33

NEROSIA LTD

Cyprus, 3025, Limassol, 63 Agias Filaxeos

December 29, 2016

Commercial INVOICE 108

Customer:
Vantage Intelligence Ltd

Description of services:

Consulting

Total amount: 20,000€.

Account: EUR/50026940689/NEROSIA LTD
IBAN : MT39STBA19116000200050026940689
Bank: SATABANK P.L.C.
BIC/SWIFT: STBAMTMT

NEROSIA LTD.

Karaiskaki, 21, Oasis Center, 2nd Floor, Flat/Office 22,
3032, Limassol, Cyprus

June, 26th, 2018

Commercial Invoice no.153

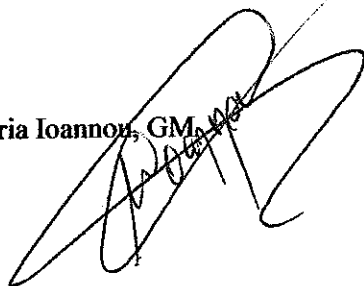
Customer:
VANTAGE INTELLIGENCE LTD.

Description of services:
Consulting Services

Total amount: 5,000 €

Please forward funds to the bank below:
- Account: EUR / 50026940689 / NEROSIA LTD
- IBAN: GB68MPOS00996300993956
- Bank: SATABANK P.L.C
- BIC/SWIFT: MPOSGB2L

Prepared by: Maria Ioannou, GM



EXHIBIT

34

From: poul kremer <bonbonic12@gmail.com>
Sent: Thursday, December 1, 2016 12:58:49 PM
Subject: Invoice
To: DS Project <dsprojectrussia@gmail.com>
Invoice N 104 - Vantage Intelligence Ltd.pdf

Dear Gretchen,

Please see attached the invoice.

Bank Details:
NEROSIA LTD

Address: Cyprus, 3025, Limassol, 63 Agias Filaxeos.

Account: EUR / 50026940689 / NEROSIA LTD
IBAN: MT39STBA19116000200050026940689
Bank: SATABANK P.L.C.
BIC/SWIFT: STBAMTMT

Best Regards!

AZ-00185612

Sent: Thur 12/29/2016 11:16:37 AM (UTC)
Subject: Invoices
From: poul kremer <bonbonic12@gmail.com>
To: DS Project <dsprojectrussia@gmail.com>
[Invoice N 107 - Vantage Intelligence Ltd.pdf](#)
[Invoice N 108 - Vantage Intelligence Ltd.pdf](#)

Dear Gretchen,

Please see attached the invoices.

Bank Details:

- NEROSIA LTD
- Address: Cyprus, 3025, Limassol, 63 Agias Filaxeos
- Account: EUR/50026940689/NEROSIA LTD
- IBAN : MT39STBA19116000200050026940689
- Bank: SATABANK P.L.C.
- BIC/SWIFT: STBAMTMT

Best Regards!

AZ_00096136

Sent: Tue 3/21/2017 1:09:01 PM (UTC)
To: "gk@vantageintel.com" <gk@vantageintel.com>
From: Nerosia <Nerosia@protonmail.com>
Subject: Invoice
Invoice N 117 - Vantage Intelligence Ltd.pdf

Dear Madam,

Please see attached invoice.

Best Regards!

AZ_00285953

Sent: Mon 4/24/2017 7:38:41 AM (UTC)
To: "gk@vantageintel.com" <gk@vantageintel.com>
From: Nerosia <Nerosia@protonmail.com>
Subject: Invoice
Invoice N 123 - Vantage Intelligence Ltd.pdf

Dear Madam,

Please see attached invoice.

Best Regards!

AZ-00252940

Sent: Mon 4/24/2017 7:39:49 AM (UTC)
To: "gk@vantageintel.com" <gk@vantageintel.com>
From: Nerosia <Nerosia@protonmail.com>
Subject: Invoice
Invoice N 124 - Notional Holdings Ltd.pdf

Dear Madam,

Please see attached invoice.

Best Regards!

A2-00252995

Sent: Wed 10/18/2017 2:35:54 PM (UTC)
Subject: Nerosia - Invoices - February-September 2017
From: Nerosia Ltd <nerosialtd@gmail.com>
To: Monica Marathefti <monica@auditnet.com.cy>

Invoice N 114 - [REDACTED]
Invoice N 115 - [REDACTED]
Invoice N 116 - Notional Holdings Ltd.pdf
Invoice N 117 - Vantage Intelligence Ltd.pdf
Invoice N 118 - [REDACTED]
Invoice N 119 - [REDACTED]
Invoice N 120 - [REDACTED]
Invoice N 121 - [REDACTED]
Invoice N 122 - [REDACTED]
Invoice N 123 - Vantage Intelligence Ltd.pdf
Invoice N 124 - Notional Holdings Ltd.pdf
Invoice N 125 - [REDACTED]
Invoice N 125 - [REDACTED]
Invoice N 126 - [REDACTED]
Invoice N 127 - [REDACTED]
Invoice N 128 - [REDACTED]
Invoice N 129 - Vantage Intelligence Ltd.pdf
Invoice N 130 - Vantage Intelligence Ltd.pdf
Invoice N 131 - [REDACTED]
Invoice N 132 - Vantage Intelligence Ltd.pdf

Dear Monica,

Please see attached invoices for February-September 2017

Best Regards,
Aviram

AZ_00591172

Sent: Tue 8/28/2018 9:42:30 AM (UTC)
Subject: Invoices
From: Nerosia Ltd <nerosialtd@gmail.com>
To: Monica Marathefti <monica@auditnet.com.cy>

Invoice N 143 - [REDACTED]
Invoice No 144 - [REDACTED]
Invoice N 141 - Vantage Intelligence Ltd.pdf
Invoice No 145 - [REDACTED]
Invoice N 142 - Vantage Intelligence Ltd.pdf
Invoice No 149 - Vantage Intelligence (Signed).v1.pdf
Invoice No 148 - [REDACTED]
Invoice No 147 - [REDACTED]
Invoice No 146 - [REDACTED]
Invoice No 151 - [REDACTED]
Invoice No 150 - [REDACTED]
Invoice No 152 - [REDACTED]
Invoice No 153 - Vantage Intelligence (Signed).pdf
Invoice No 154 - [REDACTED]
Invoice No 155 - [REDACTED]
Invoice No 157 - [REDACTED]
Invoice No 156 - [REDACTED]
Invoice No 159 - [REDACTED]
Invoice No 158 - [REDACTED]
Invoice No 160 - [REDACTED]

Hi Monica,
Please find enclosed revenues Commercial Invoices up until today
Please pay attention to the fact that some of the invoices were canceled
Regards,
Aviram

AZ_00591738

EXHIBIT

35

Notional Holdings Limited

Invoice

Invoice No: 10040

Bill To:

Mojave East Management Pte Limited
Heritage House
PO Box 889
235 Main Street
Gibraltar

Date

16 March 2015

Description

Total

Fee for M. Shvetsova re work on RC Data collection and Jervis

USD 75,000

VP Bank (Switzerland) Ltd

Bahnhofstrasse 3

Zurich CH-8022

Account Name: Notional Holdings Ltd

IBAN (USD): CH61 0853 4102 0972 8000 4

Swift code: VPBVCHZH

Total

USD 75,000

Mariya Shvetsova

Bill to: Mojave East Management Pte
Limited
Heritage House
PO Box 889
235 Main Street
Gibraltar

Date: March 9, 2015

Invoice ID: MS20153001

Description	Amount
Consulting fee: investigative services	USD 75,000
Expenses:	USD 0

Payment by wire transfer:

CFM Monaco
Address: 11 Boulevard Albert 1er
MC 98000 Monaco
IBAN: MC58 1273 9000 7005 3361 0000 019
BIC CODE: CFMOMCMXXX

Total Due: USD 75,000

EXHIBIT

36

<u>USDOJ BATES</u> <u>NUMBER</u>	<u>DATE</u>	<u>TIME</u>	<u>To</u>	<u>From</u>	<u>Subject</u>
AZ_00081494	1/19/2016	11:08:35 GMT	feldman23@gmail.com	Twitter	We've received report abuse on one of your Twitter Post
AZ_00873654	3/3/2017	12:11:33 PM (UT)	feldman23@gmail.com	LinkedIn	Shawne Fielding visited your profile 7 times
AZ_00873736	3/3/2017	12:26:38 PM (UT)	feldman23@gmail.com	LinkedIn	Richard Graham visited your profile 2 times
AZ_00634704	3/6/2017	7:49:19 AM (UTC)	feldman23@gmail.com	YouPorn	You have been successfully subscribed to Youporn.com
AZ_00634711	3/6/2017	8:43:37 AM (UTC)	feldman23@gmail.com	YouPorn	Hot blond wife gangbangd by plenty of men
AZ_00634718	3/6/2017	8:44:30 AM (UTC)	feldman23@gmail.com	YouPorn	Private Casting X - She loves sucking balls
AZ_00634725	3/6/2017	8:45:01 AM (UTC)	feldman23@gmail.com	YouPorn	Tina Got Fucked For The First Time WATCH DE
AZ_00634730	3/6/2017	8:45:29 AM (UTC)	feldman23@gmail.com	YouPorn	Sexy Big Boobs MILF Swallows Young Cock in 5ta
AZ_00634777	3/6/2017	9:13:26 AM (UTC)	feldman23@gmail.com	David Rourke	Please keep confidential as I still have to present to
AZ_00634790	3/6/2017	9:18:00 AM (UTC)	feldman23@gmail.com	Elsa Antoniou	Elsa Antoniou shared Latest Photoshoot with you
AZ_00634821	3/6/2017	9:41:59 AM (UTC)	feldman23@gmail.com	Gary Carr	Please see the attached document for a copy of a cover letter of Delphi Management Limited.
AZ_00635745	3/7/2017	6:15:14 AM (UTC)	feldman23@gmail.com	Fielding Shawne on Face	Fielding Shawne is waiting for you to see her post on your timeline "Got a little sun today"
AZ_00636237	3/7/2017	9:36:02 AM (UTC)	feldman23@gmail.com	Xvideos	Your account was created. Thank you for joining us.
AZ_00636362	3/7/2017	9:50:18 AM (UTC)	feldman23@gmail.com	Xvideos	Dirty Flix - Seduced by mature porn agent
AZ_00636373	3/7/2017	9:51:37 AM (UTC)	feldman23@gmail.com	Xvideos	Female Fake Taxi Reporter receives hot sex sc
AZ_00636383	3/7/2017	9:52:27 AM (UTC)	feldman23@gmail.com	Xvideos	Lora row gives pov blowjob in the casting. Tami
AZ_00636396	3/7/2017	9:53:16 AM (UTC)	feldman23@gmail.com	Xvideos	Awesome Breasts Blonde Teen Cracker Blows A
AZ_00636409	3/7/2017	9:53:55 AM (UTC)	feldman23@gmail.com	Xvideos	Corking hot and seductive pretty girl
AZ_00636419	3/7/2017	9:54:32 AM (UTC)	feldman23@gmail.com	Xvideos	ATTACKING THE PUSSY LIKE IT STOLE SOME
AZ_00636429	3/7/2017	9:55:15 AM (UTC)	feldman23@gmail.com	Xvideos	She s A Real Go Getter
AZ_00636849	3/7/2017	12:18:51 PM (UT)	feldman23@gmail.com	Facebook Assistance Tea	Confirm your email address
AZ_00636251	3/10/2017	6:54:13 AM (UTC)	feldman23@gmail.com	Xvideos	Your account was created. Thank you for joining us.
AZ_00636353	3/10/2017	6:55:56 AM (UTC)	feldman23@gmail.com	Xvideos	Naughty Wifey Shocked By His Size
AZ_00636367	3/10/2017	6:56:26 AM (UTC)	feldman23@gmail.com	Xvideos	PJGIRLS Sweet Lollipop - Lick and taste Lola s
AZ_00636380	3/10/2017	6:57:11 AM (UTC)	feldman23@gmail.com	Xvideos	Fitness Rooms Petite ballet teachers secret threesome
AZ_00636393	3/10/2017	6:57:38 AM (UTC)	feldman23@gmail.com	Xvideos	Ass Spitting and Milking Compilation - Girls Rim
AZ_00636404	3/10/2017	6:58:04 AM (UTC)	feldman23@gmail.com	Xvideos	BBW Fucks Pussy Hard
AZ_00636425	3/10/2017	6:58:33 AM (UTC)	feldman23@gmail.com	Xvideos	Black Ex Girlfriend Sucks Dick And Shows of Pus
AZ_00636477	3/10/2017	7:21:47 AM (UTC)	feldman23@gmail.com	Gary Carr	Gary Carr has invited you to edit the following document
AZ_00636508	3/10/2017	7:26:48 AM (UTC)	feldman23@gmail.com	Gary Carr	Gary Carr has shared a folder with you
AZ_00636605	3/10/2017	7:50:06 AM (UTC)	feldman23@gmail.com	Google News	Delphi Management Inc. MA Purchases 9 Shares of D/B/A Chubb Limited New (CB)
AZ_00637543	3/11/2017	11:48:37 AM (UT)	feldman23@gmail.com	Google Assistance Team	Alert: could not send message for next 24 hours
AZ_00875622	3/15/2017	5:11:41 AM (UTC)	feldman23@gmail.com	Google News	Donald Trump tax: Leaked 2005 document reveals Why Letting Go, for Trump, Is No Small or Simple Task
AZ_00636730	3/22/2017	6:14:32 AM (UTC)	feldman23@gmail.com	Google News	Why Letting Go, for Trump, Is No Small or Simple Task
AZ_00636751 / USAO-					
AA_001106057	3/22/2017	6:15:06 AM	Caleb23@aol.com	Google News	"President Trump Full Speech to Congress ABC News"
AZ_00636958	3/22/2017	6:34:42 AM (UTC)	feldman23@gmail.com	YouTube	London Attack: Twenty Four dead in Westminster
AZ_00634905	3/23/2017	5:03:59 AM (UTC)	feldman23@gmail.com	Google News	Alert: could not send message for next 24 hours
AZ_00638811	3/25/2017	7:03:53 AM (UTC)	feldman23@gmail.com	Google Assistance Team	Land Reform under ANC. What's next?
AZ_00636788	3/27/2017	8:56:31 AM (UTC)	feldman23@gmail.com	Google News	Rand drops as Zuma recalls South Africa's finance minister
AZ_00637131	3/28/2017	4:45:29 AM (UTC)	feldman23@gmail.com	Google News	"South Africans Jacob Zuma could be the funniest President in Africa"
AZ_00637442	3/28/2017	5:27:11 AM (UTC)	feldman23@gmail.com	YouTube	Security alert for you linked Google account
AZ_00635756	3/30/2017	9:19:28 AM (UTC)	feldman23@gmail.com	accounts-support-ara	"Interview with Chris Reider and other senior officials
AZ_00635773	3/30/2017	9:41:43 AM (UTC)	feldman23@gmail.com	YouTube	UNSUBSCRIBE Now if you want >>
AZ_00635817	3/30/2017	11:02:50 AM (UT)	feldman23@gmail.com	YouPorn	Guy gets to sport his salty seed in her pussy
AZ_00356266	4/6/2017	12:23:58 PM (UT)	feldman23@gmail.com	YouPorn	Sucking and fucking my dildo in just my hoodie and Uggs
AZ_00356272	4/6/2017	12:26:48 PM (UT)	feldman23@gmail.com	YouPorn	Stepson Makes Busty Mom Squirt
AZ_00356316	4/7/2017	6:34:03 AM (UTC)	feldman23@gmail.com	YouPorn	David Axelrod shares "IMG_1629.JPG" with you
AZ_00356319	4/7/2017	8:46:55 AM (UTC)	feldman23@gmail.com	David Axelrod	BAEB Best of beautiful brunette babe Leah Gotti
AZ_00356327	4/7/2017	6:41:11 AM (UT)	feldman23@gmail.com	YouPorn	Sexy Sheila with her boyfriend
AZ_00356330	4/7/2017	6:46:37 AM (UTC)	feldman23@gmail.com	YouPorn	do you know Ana Correia, Joao Ferreira or Eduardo Rosas?
AZ_00356363	4/7/2017	12:55:31 PM (UT)	feldman23@gmail.com	LinkedIn	

AZ_00356360	4/10/2017	5:07:29 AM (UTC feldman23@gmail.c	Google News	NYPD Sets to Deploy 1,200 Bodycams around the City
AZ_00636509	4/13/2017	10:55:31 AM (UTC feldman23@gmail.c	Facebook Assistance Tea	We've received a report abuse on one of your posts
AZ_00636522 / USAO-				
AA_001105596	4/13/2017	10:55:48 AM	Caleb23@aol.com Facebook Assistance Tea	We've received a report abuse on one of your posts
AZ_00636562	4/13/2017	12:53:36 PM (UTC feldman23@gmail.c	Xvideos	Your recent attempt to unsubscribe from our service was incomplete.
AZ_00636581	4/13/2017	12:53:36 PM (UTC feldman23@gmail.c	Xvideos	Your recent attempt to unsubscribe from our service was incomplete.
AZ_00636563	4/17/2017	10:04:13 AM (UTC feldman23@gmail.c	Facebook Assistance Tea	Your account will be deactivated within 24 hours
AZ_00641238	4/17/2017	7:11:22 AM (UTC feldman23@gmail.c	Google	Alert: could not send message for next 24 hours
AZ_00641376	4/26/2017	5:57:59 AM (UTC feldman23@gmail.c	Google News	US installs missile defence in South Korea amid tensions with North
AZ_00636162	4/27/2017	5:11:36 AM (UTC feldman23@gmail.c	Google News	North Korea faces tighter sanctions under Trump Strategy
AZ_00636305	4/27/2017	6:27:23 AM (UTC feldman23@gmail.c	Google News	South Korean acting President Hwang Kyo-ann (centre, front) inspected a variety of firearms during
AZ_00636599	4/27/2017	8:48:12 AM (UTC feldman23@gmail.c	Google	Alert: could not send message for next 24 hours
AZ_00637809	4/28/2017	5:05:00 AM (UTC feldman23@gmail.c	Elsa Antoniou	Elsa Antoniou shared an Album with you
AZ_00637990	4/28/2017	6:28:51 AM (UTC feldman23@gmail.c	YouPorn	You have been successfully subscribed to Youporn.com
AZ_00637998	4/28/2017	6:33:53 AM (UTC feldman23@gmail.c	YouPorn	Multi Orgasmic Cougar Loves Rough Anal
AZ_00638049	4/28/2017	6:36:04 AM (UTC feldman23@gmail.c	YouPorn	Girlsway Mia Tribs with Uma for 18th Birthday!
AZ_00638062	4/28/2017	6:37:26 AM (UTC feldman23@gmail.c	YouPorn	Hot busty girls getting their juicy pussy licked an
AZ_00638083	4/28/2017	7:03:44 AM (UTC feldman23@gmail.c	YouPorn	Double Penetration for a hot babe
AZ_00638107	4/28/2017	7:25:10 AM (UTC feldman23@gmail.c	YouPorn	She Knows What Fuck Means - Black Market
AZ_00640851	5/1/2017	6:33:04 AM (UTC feldman23@gmail.c	PornHub	You have been successfully subscribed to Pornhub.com
AZ_00636302	5/2/2017	4:37:05 AM (UTC feldman23@gmail.c	Google News	South Africa's Jacob Zuma abandons rally after being
AZ_00636847	5/3/2017	4:34:10 AM (UTC feldman23@gmail.c	Google News	Not Zuma's responsibility to create jobs, ANC MP says
AZ_00639987	5/4/2017	4:59:38 AM (UTC feldman23@gmail.c	Google News	'Booing is democracy': Zuma tells South Africans
AZ_00640098	5/8/2017	4:50:55 AM (UTC feldman23@gmail.c	Google News	Zuma and ANC 'tasting their own medicine' from boozers, says COPE
AZ_00357602	5/12/2017	12:19:51 PM (UTC feldman23@gmail.c	Facebook	Rebecca Alessandra Giacchi tagged you in a post on Facebook: "love you sweet heart"
AZ_00359103	6/7/2017	9:35:04 AM (UTC feldman23@gmail.c	Google News	Fired FBI director Comey 'asked not be left alone
AZ_00359107	6/7/2017	9:44:27 AM (UTC feldman23@gmail.c	Google News	US officials scramble to limit Donald Trump's diplomatic damage over Qatar tweets
AZ_00358809	6/9/2017	7:01:42 AM (UTC feldman23@gmail.c	New York Post	Pregnant woman stabbed in the neck while riding
AZ_00358820	6/9/2017	7:11:09 AM (UTC feldman23@gmail.c	New York Post	UK election results hung Parliament in stunning setback for Theresa May
AZ_00358902	6/9/2017	9:57:18 AM (UTC feldman23@gmail.c	John O'Kelly	John O'Kelly-Lynch shared "UFG Private Equity Fund"
AZ_00358985	6/12/2017	11:44:43 AM (UTC feldman23@gmail.c	PornHub	You have been successfully subscribed to Pornhub.com
AZ_00359146	6/13/2017	5:45:55 AM (UTC feldman23@gmail.c	New York Post	Another federal appeals court rules against Trump's
AZ_00359147	6/14/2017	10:36:51 AM (UTC feldman23@gmail.c	New York Post	This is exactly how long sex should last
AZ_00359156	6/14/2017	10:46:28 AM (UTC feldman23@gmail.c	New York Post	Massive fire breaks out in London high-rise
AZ_00359168	6/14/2017	11:08:26 AM (UTC feldman23@gmail.c	New York Post	Trump Clears way for Pentagon to send more troops to Afghanistan
AZ_00359183	6/14/2017	11:49:05 AM (UTC feldman23@gmail.c	New York Post	Over 500,000 have applied to join first 'space nation'
AZ_00746805	11/28/2017	11:32:09 AM (UTC feldman23@gmail.c	BBC Account	Welcome to your BBC account - let's get you started
AZ_02220361	11/28/2017	11:32:09 AM (UTC feldman23@gmail.c	BBC Account	Welcome to your BBC account - let's get you started
AZ_00327330	9/7/2018	11:28:18 AM (UTC feldman23@gmail.c	Helpdesk Team	Mail delivery failed!
AZ_00185202	9/8/2018	7:40:13 AM (UTC Caleb23@aol.com	Quiz Time	Who Is Your Alter Ego? Hidden Personality Quiz
AZ_00751412	9/19/2018	9:51:37 AM (UTC feldman23@gmail.c	Premium Account (Xvideo	Account Registered
AZ_00751426	9/19/2018	10:44:49 AM (UTC feldman23@gmail.c	Premium Account (Xvideo	Top trending video for you
AZ_00751461	9/21/2018	6:24:43 AM (UTC feldman23@gmail.c	PornHub	+18 videos sharing to your social media accounts.
AZ_00751490	9/27/2018	7:41:17 AM (UTC feldman23@gmail.c	XVIDEOS	Action Required
AZ_00751510	10/3/2018	11:50:24 AM (UTC feldman23@gmail.c	PornHub	Latest videos all around the world
AZ_00751520	10/6/2018	12:03:47 PM (UTC feldman23@gmail.c	PornHub	Some stuff from Pornhub.
AZ_00751525	10/6/2018	12:16:20 PM (UTC feldman23@gmail.c	PornHub	Most watched video in 24 hours.
AZ_00751140	10/12/2018	6:06:36 AM (UTC feldman23@gmail.c	Xvideos	Update your account preferences
AZ_00751140 / USAO-	10/24/2018	3:50:57 AM	Caleb23@aol.com Adult Tips	Things to know ever before giving blowjob

<u>USDOJ BATES NUMBER</u>	<u>DATE</u>	<u>TIME</u>	<u>PAGES</u>	<u>TO</u>	<u>FROM</u>	<u>SUBJECT</u>
AZ_00636751 / USAO-AA_001106057	3/22/2017	6:15:06 AM	2	Caleb23@aol.com	Google News	Why Letting Go, for Trump, Is No Small or Simple Task
AZ_00636522 / USAO-AA_001105596	4/13/2017	10:55:48 AM	1	Caleb23@aol.com	Facebook Assistance Team	We've received a report abuse on one of your posts.
AZ_00185202	9/8/2018	7:40:13 AM (UTC)	1	Caleb23@aol.com	Quiz Time	Who Is Your Alter Ego? Hidden Personality Quiz
AZ_00751705 / USAO-AA_001427433	10/24/2018	3:50:57 AM	3	Caleb23@aol.com	Adult Tips	Things to know ever before giving blowjob

EXHIBIT

37

From: **David Rourke** shareddrivefile@gmail.com
Subject: **Yukos Capital SARL Details**
Date: **Jan 29, 2019 at 4:58:20 AM**
To: **feldman23@gmail.com**

David Rourke has sent you an email via Gmail confidential mode:

 **Yukos Capital SARL Details**

This message was sent on January 29, 2019

[View the email](#)



From: **David Rourke** David@delphi.bm
Subject: **RE: DoAA, 2004 Security Trust to TSDT - executed**
Date: **Jan 29, 2019 at 9:59:01 AM**
To: **Daniel Feldman** feldman23@gmail.com

Daniel,

No, I did not. SPAM I imagine.

Regards
David

From: Daniel Feldman [mailto:feldman23@gmail.com]
Sent: Tuesday, January 29, 2019 10:54 AM
To: David Rourke <David@delphi.bm>
Subject: Re: DoAA, 2004 Security Trust to TSDT - executed

David:

Did you send me a document on a shared drive today?

EXHIBIT

38

MALTIN LITIGATION SUPPORT

Daniel:

UTC timestamp	Target Email	Spoofed Sender	Subject Line
1/13/16 12:45	caleb23@ao l.com	"Twitter" noreply-mails@twitter.com	Teri Lindeberg sent you a Direct Message.
1/14/16 5:44	caleb23@ao l.com	failmailurennotice@tech-center. com	Mail failure notice
1/14/16 6:58	Feldman23 @gmail.com	failmailurennotice@tech-center. com	Mail failure notice
1/19/16 11:11	Feldman23 @gmail.com	"Twitter" info@twitter.com	We've received report abuse on one of your Twitter Post
1/19/16 11:12	feldmand@ yukos.ru	"Twitter" info@twitter.com	We've received report abuse on one of your Twitter Post
2/15/16 11:31	Feldman23 @gmail.com	"LinkedIn" noreply-daily-update@linkedin. com	Daniel, confirming your email address will give you full access to LinkedIn
4/9/16 7:13	caleb23@ao l.com	info.security@twitter.com	We've received a report abuse on one of your posts.
4/9/16 7:19	caleb23@ao l.com	"Twitter" info.security@twitter.com	
3/16/17 7:24	feldman23 @gmail.com	"GARY CARR" Garv@delphi.bm	GARY CARR shared "New delphi Management Limited Policies.pdf" with you
3/30/17 6:30	feldman23 @gmail.com	"Gary Carr" gary@delphi.bm	Please find the attached document of notice.
3/30/17 7:05	caleb23@ao l.com	"Gary Carr" gary@delphi.bm	Please find the attached document of notice.
3/30/17 7:22	caleb23@ao l.com	"Google News" news.notification@mail.com	Crude spill hits Venezuela oil port, exports unaffected
3/30/17 7:27	feldman23 @gmail.com	"Google News" news.notification@mail.com	Crude spill hits Venezuela oil port, exports unaffected
3/30/17 9:54	feldman23 @gmail.com	"Gary Carr" gary@delphi.bm	Confidentials
3/31/17 7:15	Feldman23 @gmail.com	"David Rourke" David@delphi.bm	Confidentials

EXHIBIT

39

MARTIN LITIGATION SUPPORT

Hacking investigation

Preliminary report

10th June 2024



MALTIN LITIGATION SUPPORT

Introduction

We have now received data from Reuters for the following individuals and their associates:

Richard Deitz
Daniel Feldman
Stephen Lynch
Dmitri Merinson

We have also received shell casings for phishing emails sent to two of Richard's colleagues at VR Capital: Eugenia Lipilina, and Marina Nacheva.

Similarly, we have also received shell casings from Reuters for individuals associated with Stephen/Monte Valle, Victoria Lynch and Oleg Vasilyev.

Reuters do not have any shell casings in respect of "Robert Foresman", but if Bob could give us any email addresses he had at the time which would not show up for searches of his name then we can search the data for those.

Similarly, there are no shell casings in the current Reuters data for Jamison Firestone at FD Advisory, but his associate Andrey Sandakov at FDS Law was spear phished at least twice.

Initial Analysis

Based on the data we currently possess, Stephen Lynch and Oleg Vasilyev, both of Monte Valle, have been sent a large number of phishing emails. The Reuters data alone outlines 179 phishing and spear phishing emails sent to Stephen. His colleague Oleg received 84 phishing and spear phishing emails. The email ID victoria.lynch@gmail.com also received one spear phishing email.

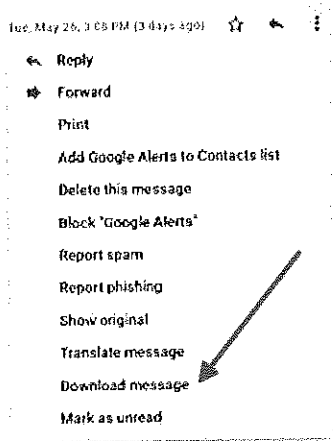
The data also includes two spear phishing attempts to Richard, eight spear phishing attempts to Marina Nacheva, and one to Eugenia, making 11 known spear phishing attempts so far on VR Capital and their associates.

The Reuters data reveals 20 spear phishing emails to Daniel and at least one to Dmitri thus far.

We have compared these shell casings with our database of publicly available shell casings from Azima, as well as non-publicly available shell casings from confidential clients, and isolated multiple "couplets", where an email from the same spoofed sender ID is sent out to different targets.

MALTIN LITIGATION SUPPORT

right of the message) and click "Download message." That should prompt you to save a .eml file. As before, put the emails into a folder on your desktop and then send them on.



Reuters shell casings

Additionally, it would be helpful if each of you would search your inboxes for the following specific emails, which are included in the Reuters whistleblower data, as set out below in their entirety, in the form received:

Richard & VR Capital:

UTC timestamp	Target Email	Spoofed Sender	Subject Line
2/9/16 6:10	rdeitz@vr-capital.com	Business_services@mail.com	RE : Thank you.
5/23/18 5:00	rdeitz@vr-capital.com	"Donot Reply" donotreplyusback@server-info.com	

2/9/16 6:15	elipilina@vr-capital.com	cwla_team@workmail.com	Re : CWLA
2/10/16 6:00	mnacheva@vr-capital.com	cwla_team@workmail.com	Re : CWLA
2/10/16 6:09	mnacheva@vr-capital.com	admin@vr-capital.com	Returned mail: see transcript for details
2/10/16 6:41	mnacheva@vr-capital.com	noreply@vr-capital.com	Returned mail: see transcript for details

MALTIN LITIGATION SUPPORT

2/10/16 9:47	marina.nacheva@gmail.com	cwla_team@workmail.com	Re : CWLA
2/12/16 11:15	marina.nacheva@gmail.com	infoalert.managementdelegate@gmail.com	Verification Required for email
2/15/16 7:40	marina.nacheva@outlook.com	Business_services@mail.com	RE : Thank you.
2/15/16 11:25	marina.nacheva@gmail.com	noreply.activitydetected@gmail.com	Confirmation Required for the account marina.nacheva@gmail.com
2/19/16 12:26	marina.nacheva@gmail.com	alert+notifications-noreply@linkedin.com	Marina, please add me to your LinkedIn network

Stephen & Monte Valle:

UTC times tamp	Target Email	Spoofed Sender	Subject Line
3/16/ 15 10:02	stephenlync h@yahoo.com	DAEMON.MAILER@yahoo.com DAEMON.MAILER@yahoo.com	
3/26/ 15 10:03	stephenlync h@yahoo.com	"=?UTF-8?B?WdCwaNC+OL4h?=" noreply-services@yahoo-inc.com	
3/30/ 15 10:39	stephenlync h@yahoo.com	DAEMON.MAILER@yahoo.com DAEMON.MAILER@yahoo.com	
12/3/ 15 7:09	slync h@monte-v	mailer-daemon@tech-center.com	Mail Failure Notice

MALTIN LITIGATION SUPPORT

	alle.s g			
12/3/ 15 7:10	slync h@mon te-v alle.c om	mailer-deamon@tech-c enter.com	Mail Failure Notice	
12/3/ 15 7:57	slync h@mon te-v alle.s g	no.reply.i.cloud.com.zjkluiyerikd383748kjhvgnt@outlook.com	Your iCloud storage is almost full.	
12/8/ 15 14:19	slync h@mon te-vall e.sg	"=?UTF-8?B?TGlua2VkSW7I hKlgVXBkYXRlcw==?="	Kim McMurray sent you a private message on LinkedIn.	
12/9/ 15 10:20	slync h@mon te-vall e.com	noreply-1linked1n-update s.notifications@post.com	YouPorn: You have been successfully subscribed YouPorn services.	
12/9/ 15 13:32	slync h@mon te-vall e.com	"Sam Steyer via YouTube" noreply.latestupdates.tub e.com@post.com	Sam Steyer sent you a video: "Money Rules Are 'Distorting' U.S. Politics: Tom Steyer"	
12/9/ 15 14:15	slync h@mon te-vall e.com	"LinkedIn Updates" noreply.jdt6rdghh1linked 1nhdhysjudfgsfw312lss @mail.com	Teresa L. Carlson viewed your profile 6 times on LinkedIn.	
12/10 /15 7:14	victori a.lync h@gm ail.co m	"Facebook" notification+zj4za2css=c 2c@facebookmail.com	We've received a report abuse on one of your posts.	
12/10 /15 7:40	slync h@mon te-vall e.com	"YouPorn Daily Love Dose" noreply.mailletters.adult.y ouporn.com@usa.com	He ends up with some bang Your daily love dose Youporn	

MALTIN LITIGATION SUPPORT

12/10 /15 8:20	steph enplyn ch@y ahoo. com	"The Moscow Times" noreply.mk.ru.newletters. russian@email.com	U.S. businessman Stephen Lynch may get into trouble soon	
12/10 /15 9:01	slynch @mon te-vall e.sg	"Apple" no-reply.icloudstorageale rt@apple.com	Your iCloud storage is almost full.	
12/10 /15 9:50	slynch @mon te-vall e.sg	"Victoria Lynch (via Google Drive)" no-reply.alerts.doc@goo glemail.com	Victoria Lynch has shared the following document	
12/10 /15 10:03	slynch @mon te-vall e.sg	"The Moscow Times" noreply.mk.ru.newletters. russian@email.com	U.S. businessman Stephen Lynch may get into trouble soon	
12/10 /15 10:24	slynch @mon te-vall e.sg	"Apple" no-reply.icloudstorageale rt@apple.com	Your iCloud storage is almost full.	
12/11 /15 6:45	slynch @mon te-vall e.sg	"YouPorn Daily Love Dose" noreply.mailletters.adult.y ouporn.com@usa.com		
12/11 /15 6:49	slynch @mon te-vall e.sg	"YouPorn Daily Love Dose" love-dose.hardcorefun@ youporn.com	He ends up with some bang Your daily love dose Youporn	
12/11 /15 6:56	slynch @mon te-vall e.sg	"YouPorn Daily Love Dose" love-dose.hardcorefun@ youporn.com	Big Dick Rough Fun Threesome Your daily love dose Youporn	
12/11 /15 12:53	slynch @mon te-vall e.sg	"YouTube" no-reply.4298035tube40 sn02=034@post.com	Finland Group Nudity, nude, erotic Girls: December Festive Party	

MALTIN LITIGATION SUPPORT

12/11 /15 19:03	slynch@monte-vall.es.g	no.reply.i.cloud.com.zjkluiyertkd383748kjhvgnt@outlook.com		Reminder::Your iCloud storage is almost full.
12/12 /15 4:36	slynch@monte-vall.es.g	"LinkedIn" message-noreply-notify@linkedin.com	Diana Klein sent you a private message on LinkedIn.	
12/12 /15 4:37	slynch@monte-vall.es.com	"LinkedIn" message-noreply-notify@linkedin.com	Diana Klein sent you a private message on LinkedIn.	
12/12 /15 4:38	stephenlynch@yahoo.com	"LinkedIn" message-noreply-notify@linkedin.com	Diana Klein sent you a private message on LinkedIn.	
12/12 /15 7:35	slynch@monte-vall.es.g	"The Moscow Times" noreply.mk.ru.newletters.russian@email.com	Stephen Lynch: This may be the end of US Businessman big empire	
12/12 /15 9:24	slynch@monte-vall.es.g	"Victoria Lynch (via =?UTF-8?B?R29vZ2xl4oSilERyaXZlKQ==?=" no-reply.alert.doc@googl email.com	Victoria Lynch	
12/12 /15 12:15	slynch@monte-vall.es.g	"YouPorn Daily Love Dose" love-dose.hardcorefun@youporn.com	Fucking Rough Threesome Your daily love dose Youporn	
12/12 /15 12:19	slynch@monte-vall.es.g	"YouPorn Daily Love Dose" love-dose.hardcorefun@youporn.com	Abusing And Spanking Rough Your daily love dose Youporn	

MALTIN LITIGATION SUPPORT

12/12 /15 12:23	slync h@m onte-v alle.s g	no.reply.apple.com.zjkluiyertkd383748kjhvgnt@outlook.com		Please make sure that we have the right address for you.
12/12 /15 13:21	slync @mon te-vall e.sg	"Money Market" noreply.newsletters.mar ketwatch.com@email.co m	Fitch Affirms TMI's Ratings	
12/14 /15 8:07	slync @mon te-vall e.sg	"The Moscow Times" noreply.newupdates.the moscowtimes.com@mail .com	Russia's Budget Deficit to Reach \$21Bln in 2016 =?UTF-8?B?4oCTIEZpbmFu?= =?UTF-8?B?Y2UgTWluaXN0cnk=?=	
12/14 /15 10:44	slync h@m onte-v alle.s g	n0-reply.lovedose_latst plusteigheten@post.co m	Rogh Gay Anal Sex Your daily love dose Youporn	
12/14 /15 11:48	slync h@m onte-v alle.s g	alyona.kovalski@minis ter.com	Important Leaked Documents	
12/22 /15 8:40	slync @mon te-vall e.com	"Evgeny Kurbanov" kurbanov_eb@dekogrou p.ru	Fwd FW: US businessman Stephen Lynch may get in trouble soon.Look it.	
12/23 /15 10:07	slync @mon te-vall e.sg	"Monte Valle" mail.failure@tech-center. com	Mail Could not be sent.	
12/23 /15 10:08	slync @mon te-vall e.com	"Monte Valle" mail.failure@tech-center. com	Mail Could not be sent.	

MALTIN LITIGATION SUPPORT

12/23 /15 10:10	steph enplyn ch@y ahoo. com	"Monte Valle" mail.failure@tech-center. com	Message left on server.	
12/24 /15 17:50	slynch @mon te-vall e.sg	"Mailer Deamon" mail.failure@tech-center. com	Reminder: Mail could not be sent.	
12/24 /15 17:52	slynch @mon te-vall e.com	"Mailer Deamon" mail.failure@tech-center. com	Reminder: Mail could not be sent.	
12/24 /15 17:53	steph enplyn ch@y ahoo. com	"Mailer Deamon" mail.failure@tech-center. com	Reminder: Mail could not be sent.	
12/24 /15 18:05	slynch @mon te-vall e.sg	"LinkedIn" message-noreply-notify @linkedin.com	We have received a report abuse for your LinkedIn account	
12/26 /15 6:26	slynch @mon te-vall e.sg	"Mail Delivery Subsystem" message.failure.notification center@tech-center.com	Delivery to the following recipient failed permanently	
12/26 /15 9:53	slynch @mon te-vall e.sg	"YouTube" noreply.you.tube.mail.ne wletters.jdusf67w87ehbd @email.com	Robert Downey Jr. pardoned for drug conviction	
12/26 /15 11:53	slynch @mon te-vall e.sg	"YouPorn" love-dose.hardcorfun@y ouporn.com	Your daily love dose Youporn Take good care of your wives!!!	
12/26 /15 12:30	slynch @mon te-vall e.sg	"LinkedIn" message-noreply-notify @linkedin.com	Teresa L. Carlson sent you a private message on LinkedIn.	

MALTIN LITIGATION SUPPORT

12/29 /15 7:39	slynch @mon te-vall e.sg	"Mailer Daemon" mailer-no.reply-message s@tech-center.com	Message could not be sent.	
12/29 /15 10:43	slynch @mon te-vall e.sg	"The Guardian" noreply.newsletters@the guardian.com	Russia warns it will retaliate after assets seized in Yukos case	
12/29 /15 12:51	slynch @mon te-vall e.sg	"The Moscow Times" noreply.newsletters@the moscowtimes.com	Yukos Shareholders may get in trouble for Compensation Case to Continue	
12/29 /15 13:11	steph enplyn ch@y ahoo. com	"Facebook" notification+zj4z2css=c2 c@facebookmail.com	=?UTF-8?B?0JDQu9C10LrRgdCw0L3QtNG AINCa0L7RgNC90LjQu9C+0LlgY29tbWVud GVk?= =?UTF-8?B?IG9uIHlvdXlgcG9zdC4=?=	
12/30 /15 10:56	steph enplyn ch@y ahoo. com	"Facebook" notification+zj4z2css=c2 c@facebookmail.com	Your photo was reported.	
12/30 /15 11:18	slynch @mon te-vall e.com	"Mail Delivery Subsystem" mail.failure@tech-center. com	Delivery to the following recipient failed permanently:	
12/30 /15 11:57	slynch @mon te-vall e.sg	"Microsoft Account Team" do-not-reply@outlookwe b.com	Message left on server : "Last night..."	
12/31 /15 5:31	slynch @mon te-vall e.com	"YouPorn" love-dose.hardcorfun@y ouporn.com	Your daily love dose Youporn Adam for Adam!!	
12/31 /15 6:09	steph enplyn ch@y	"YouPorn" love-dose.hardcorfun@y ouporn.com	You have been successfully subscribed to Youporn.com	

MALTIN LITIGATION SUPPORT

	ahoo. com			
12/31 /15 6:13	steph enplyn ch@y ahoo. com	"YouPorn" love-dose.hardcorfun@y ouporn.com	Your daily love dose Youporn Adam for Adam!!	
12/31 /15 6:53	slync h@mon te-vall e.sg	"Picasa Web Albums" no-reply.alerts.picasa@g ooglemail.com	Lukas Casey added 10 photos to album Happy New Year 2016....hahahaha!!!	
12/31 /15 7:37	steph enplyn ch@y ahoo. com	"Facebook" notification+zj4z2css=c2 c@facebookmail.com	Your photo was reported	
12/31 /15 7:42	steph enplyn ch@y ahoo. com	"Yandy Deals" =?UTF-8?B?8J+SjA==?=" services@yandi.com	Special offer! Get Lingerie In Only \$2 ! Use Your Promotional Code NOW =?UTF-8?B?8J+SjCDwn46J?="	
1/2/1 6 13:46	steph enplyn ch@y ahoo. com	"YouPorn" love-dose.hardcorfun@y ouporn.com	Your daily love dose Youporn Give everything to get everything!!!	
1/3/1 6 9:12	slync h@m onte-v alle.s g	robert.klein@europe.c om	Mail Failure Notice	
1/4/1 6 7:32	steph enplyn ch@y ahoo. com	"YouPorn" love-dose.hardcorfun@y ouporn.com		
1/4/1 6 8:11	steph enplyn ch@y ahoo. com	love-dose.hardcorfun @youporn.com	Your daily love dose Youporn Fast and Furious!!!!	

EXHIBIT 40



Claim No. HC-2016-002798

HC-2016-002798

IN THE HIGH COURT OF JUSTICE

BUSINESS AND PROPERTY COURTS OF ENGLAND AND WALES

BUSINESS LIST (ChD)

25 March 2024

BEFORE MR JUSTICE MICHAEL GREEN (the Assigned Judge)

B E T W E E N:

RAS AL KHAIMAH INVESTMENT AUTHORITY

Claimant / Defendant to Counterclaim

-and-

FARHAD AZIMA

Defendant / Counterclaimant

-and-

DAVID NEIL GERRARD

Second Additional Defendant to Counterclaim

-and-

DECHERT LLP

Third Additional Defendant to Counterclaim

-and-

JAMES EDWARD DENNISTON BUCHANAN

Fourth Additional Defendant to Counterclaim

ORDER

UPON the Claimant and Defendant to Counterclaim (“**RAKIA**”) bringing proceedings against the Defendant and Counterclaimant (“**Mr Azima**”) by a claim form issued on 30 September 2016 (and the claim thereby brought being repeatedly amended) (“**RAKIA’s Claim**”);

AND UPON Mr Azima being granted permission to bring a counterclaim against RAKIA by the order of HHJ Kramer sealed on 13 August 2019 (the “**First Counterclaim**”), and the Court

thereby further ordering that the First Counterclaim was to be stayed following service of the pleading containing the First Counterclaim on RAKIA;

AND UPON the Court (Mr Andrew Lenon QC, sitting as a Deputy Judge of the High Court – the “**Deputy Judge**”) hearing the trial of RAKIA’s Claim between 22 January 2020 and 14 February 2020 (the “**First Trial**”);

AND UPON the judgments in [2020] EWHC 1327 (Ch) and [2020] EWHC 1686 (Ch) (together, the “**First Trial Judgments**”) and the order of the Deputy Judge dated 31 July 2020 (the “**First Trial Order**”) following the First Trial;

AND UPON Mr Azima appealing to the Court of Appeal from the First Trial Order and Judgments (the “**First Appeal**”)

AND UPON a bank account (the “**Joint Account**”) having been opened in the joint names of Burlingtons Solicitors LLP and Stewarts Law LLP (“**Stewarts**”) in accordance with paragraph 1.A. of the order of the Court of Appeal dated 9 September 2020 (the “**Appeal Permission Order**”);

AND UPON Mr Azima having caused certain sums to be paid into the Joint Account, in accordance with paragraph 1.A of the Appeal Permission Order;

AND UPON the judgment of the Court of Appeal on the First Appeal in [2021] EWCA Civ 349 (the “**First Appeal Judgment**”) and the Order of the Court of Appeal dated 15 March 2021 (the “**First Appeal Order**”) remitting Mr Azima’s counterclaim (the “**Hacking Counterclaim**”);

AND UPON the Order of Mr Justice Leech dated 21 June 2022 (the “**Leech Order**”), granting Stewarts’ without notice application under CPR 42.3 dated 20 June 2022, pursuant to which Stewarts were permitted to cease to act for RAKIA;

AND UPON RAKIA’s letter to the Court of 22 June 2022 wherein RAKIA stated that it would “*withdraw from the proceedings*”;

AND UPON the order of Mr Justice Michael Green sealed on 8 July 2022 providing that Stewarts had remained and were to remain the address for service on RAKIA until further order of the Court (the “**Service Order**”);

AND UPON the order of Mr Justice Michael Green dated 7 November 2022 (the “**Rescission Permission Order**”) which (i) granted permission for Mr Azima to amend his statement of case to bring an additional Counterclaim against RAKIA (the “**Rescission Counterclaim**”) seeking an order setting aside the First Trial Judgments and the First Trial Order and the First Appeal Judgment and (in part) the First Appeal Order on the basis that they were procured by fraud, and (ii) required RAKIA to file and serve its Re-Amended Defence by 6 December 2022;

AND UPON service of the Re-Re-Re-Amended Counterclaim and Claim Against Additional Parties (including the Rescission Counterclaim) on 8 November 2022;

AND UPON RAKIA’s failure to file an acknowledgment of service or a defence to the Rescission Counterclaim by 6 December 2022 (or at all);

AND UPON the judgment of the Court of Appeal refusing the Second, Third and Fourth Additional Defendants’ appeals against the Rescission Permission Order ([2023] EWCA Civ 507) and the order of 16 May 2023 dismissing those appeals;

AND UPON Mr Azima’s application by notice dated 6 June 2023 for default judgment against RAKIA in the Rescission Counterclaim pursuant to CPR 12.3(1) and/or CPR 12.3(2) (the “**First Rescission Application**”);

AND UPON Mr Azima’s application dated 3 July 2023 for an order striking out RAKIA’s Statement of Case in the Hacking Counterclaim, in the alternative for an ‘unless’ order, and consequential judgment on the claim (the “**Hacking Judgment Application**”);

AND UPON the Court granting the Hacking Judgment Application but refusing the First Rescission Application by order dated 3 October 2023 (the “**3 October Order**”), giving effect to a judgment delivered on 21 August 2023;

AND UPON the 3 October Order ordering RAKIA to pay Mr Azima his costs of the Hacking Counterclaim up to 6 June 2023 (without prejudice to any right that Mr Azima may have to seek costs of the Hacking Counterclaim as against the Additional Defendants in due course, subject to principles against double recovery), and listing all claims for damages or further costs against RAKIA under the Hacking Counterclaim for determination at trial of the Hacking Counterclaim;

AND UPON Mr Azima applying to vary the requirement for funds to be paid into the Joint Account under the Appeal Permission Order, and the Court of Appeal (Lewison LJ) by its order

of 15 December 2023 determining that application, varying the Appeal Permission Order and awarding Mr Azima his costs of that application on the indemnity basis, to be assessed (the **‘Joint Account Variation Order’**)

AND UPON Mr Azima and the Second and Third Additional Defendants agreeing to a settlement of the Hacking Counterclaim against the Second and Third Additional Defendants by means of acceptance (in writing on 17 January 2024) of an offer made under Part 36 of the Civil Procedure Rules, and the Second and Third Additional Defendants having agreed not to oppose any fresh or renewed application issued by Mr Azima seeking default judgment against RAKIA of the Rescission Counterclaim;

AND UPON Mr Azima and the Fourth Additional Defendant agreeing to a settlement of the Hacking Counterclaim against the Fourth Additional Defendant as recorded in a Tomlin Order sealed on 11 March 2024, and the Tomlin Order reciting the Fourth Additional Defendant’s confirmation that he will not oppose any renewed application by Mr Azima seeking default judgment against RAKIA of the Rescission Counterclaim;

AND UPON Mr Azima’s application by notice dated 19 March 2024 for default judgment against RAKIA in the Rescission Counterclaim pursuant to CPR 12.3(1) and/or CPR 12.3(2), and for the determination of remedies against RAKIA under the Hacking Counterclaim, and for costs and other relief against RAKIA (the **‘March 2024 Applications’**);

AND UPON the March 2024 Applications having been served on RAKIA;

AND UPON hearing leading counsel for Mr Azima, and RAKIA not attending the hearing of the March 2024 Applications

IT IS ORDERED THAT

1. There be judgment in default for Mr Azima and against RAKIA on the Rescission Counterclaim.
2. The First Trial Judgments and the First Trial Order are set aside.
3. The First Appeal Judgment is set aside.
4. Paragraphs 4-7 and 12-14 of the First Appeal Order are set aside.

5. Paragraph 13 of the 3 October Order is varied so as to read as follows: *“Any claims for damages or further costs (including the repayment of sums paid by Mr Azima to RAKIA in interest on damages, costs and interest on costs under paragraphs 1(b) and 3-7 of the First Trial Order) shall be listed for determination at the Pre-Trial Review to take place in a three day window on 25, 26 or 27 March 2024, and/or on such other date(s) as the Court may direct.”*
6. The following orders for costs in RAKIA’s favour are set aside: (i) paragraphs 6.2, 6.3 and 6.4 of the order of HHJ Kramer of 18 July 2018 (sealed on 25 July 2018); (ii) paragraphs 4.2 and 4.3 of the order of HHJ Kramer of 23 January 2019 (sealed on 24 January 2019). Within 14 days of this order, RAKIA is to repay all the amounts paid to it under those orders.
7. RAKIA shall pay Mr Azima’s costs of and occasioned by RAKIA’s Claim and the First Counterclaim, to be paid on the indemnity basis, with such costs to be subject to detailed assessment immediately if not agreed. RAKIA shall pay interest on those costs from the date on which they were paid by or on behalf of Mr Azima to the date of this Order at a rate of 1% per annum over the Bank of England base rate from time to time, and from the date of this order until the date the costs are paid at a rate of 8% per annum.
8. RAKIA shall pay Mr Azima’s costs of and occasioned by the First Appeal, to be paid on the indemnity basis, with such costs to be subject to detailed assessment immediately if not agreed. RAKIA shall pay interest on those costs from the date on which they were paid by or on behalf of Mr Azima to the date of this Order at a rate of 1% per annum over the Bank of England base rate from time to time, and from the date of this order until the date the costs are paid at a rate of 8% per annum. Within 14 days of this Order, RAKIA shall repay to Mr Azima the sums paid by Mr Azima under paragraph 14 of the First Appeal Order, together with interest on the same basis as in the preceding sentence.
9. RAKIA shall pay Mr Azima’s costs of and occasioned by the Rescission Counterclaim, to be paid on the indemnity basis, with such costs to be subject to detailed assessment immediately if not agreed. RAKIA shall pay interest on those costs from the date on which they were paid by or on behalf of Mr Azima to the date of this Order at a rate of 1% per annum over the Bank of England base rate from time to time, and from the date of this order until the date the costs are paid at a rate of 8% per annum.

10. RAKIA shall pay Mr Azima's costs of the Hacking Counterclaim insofar as those costs were incurred after 6 June 2023 and relate to the remedies and costs sought against RAKIA under the Hacking Counterclaim, with such costs to be subject to detailed assessment immediately if not agreed. RAKIA shall pay interest on those costs from the date on which they were paid by or on behalf of Mr Azima to the date of this Order at a rate of 1% per annum over the Bank of England base rate from time to time, and from the date of this order until the date the costs are paid at a rate of 8% per annum.
11. Within 14 days of the date RAKIA is served with this Order, RAKIA is to make the following interim payments on account of costs and interest:
 - a. The sum of £2,731,026.43 on account of the costs and interest on costs specified in paragraph 7.
 - b. The sum of £1,683,580.25 on account of the costs and interest on costs specified in paragraph 8.
 - c. The sum of £1,381,825.20 on account of the costs and interest on costs specified in paragraph 9.
12. Within 14 days of this Order, RAKIA is to pay Mr Azima damages (and interest on damages) assessed as follows:
 - a. The sum of US\$1,431,338.17 for Mr Azima's loss in financing the amounts paid into the Joint Account in order to satisfy the condition in paragraph 1A of the Permission Order.
 - b. The sum of £14,207.64 for Mr Azima's pecuniary loss.
 - c. The sum of £200,000.00 for Mr Azima's non-pecuniary loss.
 - d. The sum of £100,000.00 as exemplary damages.
 - e. The sum of £2,313.97 as interest on the pecuniary loss in paragraph 12.b.
13. RAKIA shall pay the costs of and occasioned by the March 2024 Applications, on an indemnity basis, summarily assessed at £113,789.50, within 14 days of the date RAKIA is served with this Order.
14. Within 28 days of the date of being served with this order, RAKIA is:

- a. to take all reasonable steps to remove or procure the removal of any websites, torrents, WeTransfer links or other internet sources containing statements about Mr Azima and/or providing means for this private data to be accessed by others;
 - b. to deliver up all copies of Mr Azima's private data in RAKIA's possession or the possession of RAKIA's agents.
15. The orders set out in paragraph 14 may (if so advised) be served by Mr Azima on RAKIA in an additional separate order under cover of a penal notice, in the form attached as Annex A to this order.
16. Any requirement for the order in paragraph 14 and the order and penal notice referred to in paragraph 15 to be personally served is dispensed with, subject to Mr Azima serving the order and penal notice in accordance with the Service Order.
17. Paragraph 11 of the 3 October Order is amended to state: "*RAKIA shall pay interest on the sums to be paid under paragraph 9: (i) from the date on which they were paid by or on behalf of Mr Azima to the date of this Order at a rate of 1% per annum above the Bank of England base rate from time to time; and (ii) from the date of this Order until the date of repayment at a rate of 8% per annum.*"
 - a. The date for Mr Azima to commence detailed assessment of: the costs awarded under paragraph 9 of the 3 October Order; and
 - b. the costs awarded to Mr Azima under the Joint Account Variation Order,is extended to three months from the date of this Order. Paragraph 10 of the 3 October Order (as amended by the order of Mr Justice Michael Green dated 12 March 2024) is amended accordingly.
18. This Order shall be served on RAKIA by Mr Azima.

ANNEX A – ORDER AND PENAL NOTICE

Claim No. HC-2016-002798

IN THE HIGH COURT OF JUSTICE

BUSINESS AND PROPERTY COURTS OF ENGLAND AND WALES

BUSINESS LIST (ChD)

BEFORE MR JUSTICE MICHAEL GREEN (the Assigned Judge)

B E T W E E N:

RAS AL KHAIMAH INVESTMENT AUTHORITY

Claimant / Defendant to Counterclaim

-and-

FARHAD AZIMA

Defendant / Counterclaimant

-and-

DAVID NEIL GERRARD AND OTHERS

Additional Defendants to Counterclaim

ORDER AND PENAL NOTICE

PENAL NOTICE - WARNING

IF YOU, THE WITHIN NAMED RAS AL KHAIMAH INVESTMENT AUTHORITY, NEGLECT TO OBEY THIS ORDER BY THE TIME STATED, YOU MAY BE HELD TO BE IN CONTEMPT OF COURT AND MAY BE PUNISHED BY A FINE, OR YOUR ASSETS MAY BE SEIZED, OR SUBJECT TO OTHER PUNISHMENT UNDER THE LAW

IF RAS AL KHAIMAH INVESTMENT AUTHORITY NEGLECT TO OBEY THIS ORDER BY THE TIME STATED, YOU, NASER THAFER HUSNI AL BUSTAMI, MOHAMAD SULTAN AL QADI, AND COLIN FREDERIC GLENROY CROOKSHANK (AS DIRECTORS OR OFFICERS OF THE SAID RAS AL KHAIMAH INVESTMENT AUTHORITY), MAY BE HELD TO BE IN CONTEMPT OF COURT AND MAY BE IMPRISONED OR FINED OR YOUR ASSETS MAY BE SEIZED, OR SUBJECT TO OTHER PUNISHMENT UNDER THE LAW

Definitions

1. This order uses the following terms:
 - a. “RAKIA” refers to the Ras Al Khaimah Investment Authority, the Claimant and Defendant to Counterclaim in these proceedings.
 - b. “Mr Azima” refers to Mr Farhad Azima, the Defendant and Counterclaimant in these proceedings.
 - c. References to the “websites, torrents, WeTransfer links or other internet sources” refers to the websites, torrents, WeTransfer links and internet sources described in paragraphs 71-74, and 99-100 of the Re-Re-Re-Amended Counterclaim and Claim Against Additional Parties.

Order

2. Within 28 days of the date of being served with this order, RAKIA is:
 - a. to take all reasonable steps to remove or procure the removal of any websites, torrents, WeTransfer links or other internet sources containing statements about Mr Azima and/or providing means for this private data to be accessed by others;
 - b. to deliver up all copies of Mr Azima’s private data in RAKIA’s possession or the possession of RAKIA’s agents.

EXHIBIT 41



[\[Home\]](#) [\[Databases\]](#) [\[World Law\]](#) [\[Multidatabase Search\]](#) [\[Help\]](#) [\[Feedback\]](#)

England and Wales High Court (Chancery Division) Decisions

You are here: [BAILII](#) >> [Databases](#) >> [England and Wales High Court \(Chancery Division\) Decisions](#) >> Ras Al Khaimah Investment Authority v Farhad Azima [2022] EWHC 2727 (Ch) (01 November 2022)
 URL: <http://www.bailii.org/ew/cases/EWHC/Ch/2022/2727.html>
 Cite as: [2022] EWHC 2727 (Ch)

[\[New search\]](#) [\[Printable PDF version\]](#) [\[Help\]](#)

Neutral Citation Number: [2022] EWHC 2727 (Ch)

Case No: HC-2016-002798

**IN THE HIGH COURT OF JUSTICE
 BUSINESS AND PROPERTY COURTS OF ENGLAND AND WALES
 BUSINESS LIST (Ch)
 ON REMITTAL FROM THE COURT OF APPEAL – [2021] EWCA CIV 349 (LEWISON, ASPLIN AND
 MALES LJ)**

Royal Courts of Justice, Rolls Building
 Fetter Lane, London, EC4A 1NL
 01/11/2022

Before:

MR JUSTICE MICHAEL GREEN

Between:

**RAS AL KHAIMAH
 INVESTMENT AUTHORITY**

**Claimant/
 Defendant to
 Counterclaim**

- and -

FARHAD AZIMA

**Defendant and
 Counterclaimant**

- and -

**(1) ~~STUART ROBERT PAGE~~
 (2) DAVID NEIL GERRARD
 (3) DECHERT LLP**

**Additional
 Defendants to
 Counterclaim**

(4) JAMES EDWARD DENNISTON BUCHANAN

Thomas Plewman KC, Frederick Wilmot-Smith and Sophie Bird (instructed by Burlingtons Legal LLP)
for the Counterclaimant
Fionn Pilbrow KC (instructed by Charles Fussell & Co LLP) for the Second Additional Defendant to the
Counterclaim
Roger Masefield KC, Laura Newton and Robert Harris (instructed by Enyo Law LLP) for the Third
Additional Defendant to the Counterclaim
Anthony White KC and Ben Silverstone (instructed by Kingsly Napley LLP) for the Fourth Additional
Defendant to the Counterclaim
Hearing Dates: 17 and 18 October 2022

HTML VERSION OF APPROVED JUDGMENT

Crown Copyright ©

This judgment was handed down remotely at 10.30am on 1 November 2022 by circulation to the parties or their representatives by email and by release to The National Archives.

.....
 MR JUSTICE MICHAEL GREEN

Mr Justice Michael Green:

INTRODUCTION

1. This is an application by Mr Farhad Azima, the Counterclaimant, for permission to bring an additional counterclaim against the original Claimant, Ras Al Khaimah Investment Authority (**RAKIA**), and to amend his statement of case in the form of a draft Re-Re-Amended Counterclaim and Claim Against Additional Parties (the **draft RRRACC**). The application is made pursuant to CPR 20.4(2)(b) and CPR 17.1(2)(b).
2. **RAKIA** is the sovereign wealth fund of the Emirate of Ras Al Khaimah (**RAK**), part of the United Arab Emirates. Mr Azima is a US-based businessman, principally involved in the aviation industry, who had various dealings with **RAKIA** between 2007 and 2016. Since 2016, they have been engaged in litigation against each other. **RAKIA** sued Mr Azima for fraudulent misrepresentation and conspiracy; the former was in relation to a Settlement Agreement dated 2 March 2016 between **RAKIA**, Mr Azima and his company, HeavyLift International Airlines FZC (**HeavyLift**), whereby **RAKIA** paid \$2.6 million to settle various claims (the **Settlement Agreement**); the latter in relation to payments to Mr Azima of \$400,000 and \$1,162,500 in 2011 and 2012 said to have been in respect of commission owed to Mr Azima for introducing **RAKIA** Georgia to three prospective purchasers of the Sheraton Metechi Palace Hotel in Tbilisi (the **Hotel**).
3. Mr Azima denied both claims and alleged by way of defence and counterclaim that his email accounts and data had been unlawfully hacked by **RAKIA** prior to the Settlement Agreement and the information so obtained by **RAKIA** was then used against him in **RAKIA**'s claim. He argued that **RAKIA**'s claim should be struck out for abuse of process or that the evidence should be excluded. **RAKIA** said that it was not responsible for the unlawful hacking and that it only discovered the hacked material when it was posted on the internet in August and September 2016.
4. The trial of **RAKIA**'s claim was heard by Mr Andrew Lenon QC, sitting as a deputy Judge of the Chancery Division (the **deputy Judge**). He found in favour of **RAKIA** on its claims for fraudulent misrepresentation and conspiracy. He rejected Mr Azima's hacking defence and dismissed the counterclaim. His judgment is reported at [2020] EWHC 1327 (Ch) (the **First Judgment**).

5. Mr Azima was granted permission to appeal by Arnold LJ on certain terms as to payment in of the judgment sum. The Court of Appeal (Lewison, Asplin and Males LJ) heard the appeal on 2 to 4 March 2021, and their joint judgment was delivered only a week later on 12 March 2021 (the **CA Judgment**). This is reported at [2021] EWCA Civ 349. It will be necessary to examine the CA Judgment in some detail. In short the Court of Appeal dismissed Mr Azima's appeal against RAKIA's claims but, based on new evidence in relation to RAKIA's responsibility for the hacking which the Court of Appeal admitted, it allowed the appeal on the counterclaim and remitted the counterclaim to be tried by a different judge of the Chancery Division. I am the assigned Judge to hear the remitted counterclaim and have now dealt with a number of applications in relation to it. The trial has recently been set down and is listed to commence in a 5-day window from 7 May 2024, with an estimated duration of between 8 and 10 weeks.
6. It was made clear in the CA Judgment and this was given effect in its Order dated 15 March 2022 (the **CA Order**) that whatever the outcome of the remitted counterclaim, the First Judgment and the factual findings on RAKIA's claim made by the deputy Judge "*must stand*". Accordingly when I come to hear the retrial of the counterclaim, I am not bound by the deputy Judge's factual findings on the hacking counterclaim but I cannot interfere with the findings made on RAKIA's substantive claim. I will however be able to vary the deputy Judge's orders in relation to interest and costs and consider whether damages should be ordered against RAKIA if found to be responsible for the hacking.
7. Mr Azima sought permission to appeal from the Supreme Court, it having been refused by the Court of Appeal. The principal basis for the application was that the Court of Appeal was wrong to have held, before the counterclaim had been retried, that the possible remedies available to Mr Azima did not include overturning RAKIA's judgment and/or having it struck out on the grounds of abuse of process. Some months after the application for permission had been lodged, Mr Azima sought to adduce further fresh evidence recently obtained that was said to show that RAKIA was responsible for the hacking and had concocted a false story as to its discovery of the hacked material, including perjured evidence, that was put to the deputy Judge at the trial.
8. On 28 April 2022, the Supreme Court refused permission to appeal "*because the application does not raise an arguable point of law*".
9. Now Mr Azima wishes to bring an additional counterclaim in which his cause of action is to have the First Judgment set aside on the grounds that it was procured by fraud. He has discovered yet more evidence which he says shows that a pervasive fraud was perpetrated on the Court at the original trial by or on behalf of RAKIA and that he therefore satisfies the test for permission, namely that there is a real prospect of establishing the conditions necessary to have the judgment set aside.
10. RAKIA is now no longer participating in these proceedings and has not appeared before me at this hearing. On 16 June 2022, it made an open offer to settle the counterclaim against it for \$1 million plus costs, but this was rejected by Mr Azima. Then on 22 June 2022, RAKIA wrote to the Court to say that it had withdrawn its instructions to its solicitors, Stewarts Law LLP (**Stewarts**), and that it did not intend to take any further part in the proceedings. Stewarts have come off the record for RAKIA but by my Order of 8 July 2022 a mechanism for serving RAKIA with documents was set out. So the entity against which the proposed new counterclaim is made does not appear to oppose Mr Azima being granted permission.
11. However the Additional Defendants do strongly oppose the application. On 16 July 2021 I gave permission to Mr Azima to join four Additional Defendants to the counterclaim. They are:
 - (1) Mr Stuart Page, a private investigator, who has since admitted involvement in the hacking on behalf of RAKIA and that he gave false evidence at the original trial; he has settled with Mr Azima and has provided an affidavit that supports Mr Azima's case;
 - (2) Mr Neil Gerrard, a retired solicitor and former partner of Dechert LLP; following an adverse judgment against him by Waksman J in the Commercial Court in an unrelated case brought by *Eurasian Natural Resources Corporation* on 16 May 2022 ([2022] EWHC 1138

(Comm)), he is now separately represented by Charles Fussell & Co; Mr Fionn Pilbrow KC made submissions on his behalf at the hearing;

(3) Dechert LLP, represented by Mr Roger Masefield KC leading Ms Laura Newton and Mr Robert Harris, instructed by Enyo Law LLP; and

(4) Mr James Buchanan, who was employed by companies in RAK and was authorised to undertake certain activities on behalf of RAKIA; he is represented by Mr Antony White KC leading Mr Ben Silverstone, instructed by Kingsley Napley LLP.

12. Even though the proposed new counterclaim is not brought against them, the Additional Defendants have vigorously opposed the grant of permission, principally on the basis that this would effectively be Mr Azima's third attempt to overturn the First Judgment on the grounds of fraud and that this amounts to an abuse of process, both on the finality principle and as a collateral attack on the CA Judgment. They also say that my jurisdiction is limited to what the Court of Appeal has remitted to me and that the only route that Mr Azima can use, particularly given that he is seeking also to set aside the CA Order, is to go back to the Court of Appeal under CPR 52.30 to re-open the appeal. The Additional Defendants further submit that, in any event, Mr Azima does not have a real prospect of satisfying the materiality condition required to justify the setting aside of the First Judgment and CA Order on the grounds of fraud.
13. Mr Azima is represented by Mr Thomas Plewman KC leading Mr Frederick Wilmot-Smith and Ms Sophie Bird, instructed by Burlingtons Legal LLP. He seemed to be taking a point on the standing of the Additional Defendants to object but Mr Plewman KC confirmed at the hearing that he does not submit that they have no standing; rather he says that it is surprising that they are running these objections on behalf of RAKIA.

THE APPLICATION

14. As I have said, I have dealt with a number of applications and hearings and have delivered some judgments in these proceedings, most recently on 27 May 2022 when I considered applications for security for costs and issues for disclosure – [2022] EWHC 1295 (Ch). On 1 July 2022, I heard a CMC and by my Order dated 8 July 2022 made various directions including as to how this application should be dealt with and the future involvement of RAKIA in the light of its letter dated 22 June 2022.
15. The application for permission to bring the additional counterclaim was issued on 24 June 2022. That sought an order pursuant to CPR 20.4(2)(b) that Mr Azima be granted permission to bring an additional counterclaim against RAKIA to set aside the First Judgment on the basis that it was obtained by fraud. The application notice stated that "*substantial and critical evidence of the fraud*" had been obtained in June 2022 and it showed that "*RAKIA provided substantial false evidence in support of its case against Mr Azima during the First Trial, which was an operative cause of the Deputy Judge's findings in favour of RAKIA.*" The application is supported by a 54-page nineteenth witness statement of Mr Dominic Holden, a partner of Burlingtons, Mr Azima's solicitors, dated 24 June 2022.
16. By paragraph 12 of my Order of 8 July 2022 I directed Mr Azima to provide RAKIA and the Additional Defendants with his draft RRRACC which should include both the proposed new counterclaim and "*any associated amendments proposed to the Hacking Counterclaim (in a format enabling the two types of amendment to be distinguished), by 29 July 2022.*"
17. Mr Azima did provide RAKIA and the Additional Defendants with his draft RRRACC on 29 July 2022. The Additional Defendants complain that the amendments could not be distinguished, contrary to my Order, and that it is not clear whether the draft RRRACC contains all of the amendments that Mr Azima will seek to make based on the new evidence. They also point to the fact that a letter before action has been sent to a further potential Additional Defendant, namely Mr David Hughes, who was a partner of Dechert at the material time, and whose joinder would obviously require further amendments to the RRRACC. While I see the force of these points, I do not think they affect the issues before me. Any further

amendments and/or applications for joinder may have to be dealt with in due course and are essentially aspects of efficient case management. I should say that it was agreed by all the parties that I should only deal with the permission application to bring the proposed additional counterclaim, while the application in relation to the other amendments would be left to a further CMC after delivery of this judgment.

18. On 19 August 2022, and in accordance with my Order, the Additional Defendants indicated that they objected to the application and the amendments contained in the draft RRRACC. They gave their reasons for their objections in: a witness statement of Mr Edward Allen, a partner of Enyo Law on behalf of Dechert; a witness statement of Mr Charles Fussell, partner of Charles Fussell & Co on behalf of Mr Gerrard; and a letter from Kingsley Napley to Burlingtons dated 19 August 2022 on behalf of Mr Buchanan. RAKIA has not indicated whether it consents or objects.
19. On 9 September 2022, Mr Azima filed evidence in reply in the form of the twenty- second witness statement of Mr Holden. At paragraphs 57-58 of that witness statement, Mr Azima confirmed that he "*is content to withdraw paragraphs §§168A-168C of the draft RRRACC and not to seek the business losses in these proceedings*". Those paragraphs included a claim for damages in respect of losses that Mr Azima said he has suffered to his US property development projects. The Additional Defendants had objected to these paragraphs on the grounds that they offended against the reflective loss rule.
20. On 30 September 2022, Mr Azima filed a re-amended Application Notice to clarify that: (1) in addition to seeking permission to bring the new counterclaim pursuant to CPR 20, he also seeks permission to amend the existing hacking counterclaim pursuant to CPR 17; and (2) in addition to seeking to set aside the First Judgment, he is also seeking to set aside the CA Judgment and the CA Order.

SETTING ASIDE A JUDGMENT FOR FRAUD

(a) Elements of the cause of action

21. As Lord Sumption said in *Takhar v Gracefield Developments Limited* [2020] AC 450 (*Takhar*) at [60]: "*An action to set aside an earlier judgment for fraud is not a procedural application but a cause of action*". Mr Azima could have issued separate proceedings against RAKIA relying on this cause of action. There may have been difficult obstacles to overcome in terms of serving and establishing jurisdiction in relation to RAKIA, but assuming RAKIA was effectively joined to the proceedings, it would only be RAKIA that could challenge Mr Azima's right to bring the claim on the grounds of abuse of process. The Additional Defendants would have had no standing to take the points they are running in this application. But because Mr Azima is seeking to bring the claim within the existing proceedings, they clearly do have standing, particularly in relation to consequential case management issues that might arise if permission is granted.
22. It is sensible and practical to bring the claim within the existing proceedings where the core factual issues are the same. But it seems to me that the test for permission should be the same whether the claim is advanced in existing proceedings or new proceedings. There was no dispute that the test on the application for permission is whether the new counterclaim has a real prospect of success. The other considerations in CPR 20.9, which are essentially in relation to case management, were not relied upon by the Additional Defendants as reasons for refusing permission.
23. *Takhar* is now the leading authority in this field. The majority judgments were those of Lord Kerr JSC and Lord Sumption, with whom Lord Hodge, Lord Lloyd-Jones and Lord Kitchin JJSC agreed. Lord Briggs and Lady Arden JJSC agreed in the result but delivered judgments that disagreed with some of the reasoning of the majority. The majority judgments expressly approved the summary of the principles governing applications to set aside judgments for fraud provided by Aikens LJ in *Royal Bank of Scotland plc v Highland Financial Partners LP* [2013] 1 CLC 596 (*Highland*) at [106]:

"The principles are, briefly: first, there has to be a 'conscious and deliberate dishonesty' in relation to the relevant evidence given, or action taken, statement made or matter concealed, which is relevant to the judgment now sought to be impugned. Secondly, the relevant

evidence, action, statement or concealment (performed with conscious and deliberate dishonesty) must be 'material'. 'Material' means that the fresh evidence that is adduced after the first judgment has been given is such that it demonstrates that the previous relevant evidence, action, statement or concealment was an operative cause of the court's decision to give judgment in the way it did. Put another way, it must be shown that the fresh evidence would have entirely changed the way in which the first court approached and came to its decision. Thus the relevant conscious and deliberate dishonesty must be causative of the impugned judgment being obtained in the terms it was. Thirdly, the question of materiality of the fresh evidence is to be assessed by reference to its impact on the evidence supporting the original decision, not by reference to its impact on what decision might be made if the claim were to be retried on honest evidence."

24. Lord Sumption in [67] of *Takhar* described these as "*stringent conditions*" which were required to remove "*the risk of frivolous or extravagant litigation to set aside judgments on the ground of fraud.*" In *Grant and Mumford on Civil Fraud* (2018) [38-003] the learned authors said:

"Accordingly, the circumstances in which a properly obtained judgment will be set aside for fraud are narrow and the court is assiduous to ensure that such claims are not used to harass or as the vehicle for seeking to revisit adverse judgments. A court will be assiduous to strike out such claims at an early stage".

(See also Burton J's description of the test as being "*difficult to comply with, and must rarely be permitted*" in *Chodiev v Stein* [2015] EWHC 1428 (Comm).)

25. Lord Briggs at [68] graphically described the tension inherent in actions to set aside a judgment for fraud as:

"...a bare-knuckle fight between two important and long-established principles of public policy. The first is fraud unravels all. The second is that there must come an end to litigation. I will call them the fraud principle and the finality principle."

26. The principles set out by Aikens LJ in *Highland* were an attempt to address that tension. Even though Aikens LJ referred to three principles, it is generally accepted that the third is really an elaboration of the second. The cause of action therefore has two relevant elements: the Fraud Condition and the Materiality Condition. Leech J in the recent case of *Tinkler v Esken Limited* [2022] EWHC 1375 (Ch) (*Tinkler*) referred to a third "*limb*" that "*there was new evidence before the Court (which was either not given or not disclosed in the earlier proceedings)*". That is not an issue in this case. The contentious issues in this case are around the requisite proof of the Materiality Condition and the fact that fraud had been raised at the original trial and dealt with by the Court of Appeal.

27. The Fraud Condition is relatively straightforward at this stage and I will deal later with the new evidence that has been discovered. None of the Additional Defendants argue that Mr Azima does not have a real prospect of satisfying the Fraud Condition which is that there was "*conscious and deliberate dishonesty*" on the part of RAKIA at the original trial. Insofar as the allegations of fraud are made against the Additional Defendants, they emphasised to me that they will be contesting those allegations if they are allowed to go forward but that they have not yet been required to put in their defences to them. It was therefore wrong to suggest, as Mr Plewman KC did, that they have not contested Mr Azima's factual assertions. They are only not contesting them for the purposes of this application.

28. They do, however, challenge whether Mr Azima has a real prospect of satisfying the Materiality Condition. In *Highland*, Aikens LJ said that the alleged fraudulent evidence, action, statement or concealment must have been "*an*", not "*the*", operative cause of the impugned decision. Aikens LJ then went on to put it another way: that the fresh evidence "*would have entirely changed the way in which the first court approached and came to its decision*" which seems to set quite a high bar.

29. The test for the Materiality Condition was not dealt with in *Takhar* which was principally concerned with whether the party was required to show that they could not, using reasonable diligence, have obtained the evidence of fraud that they now wished to rely on in applying to set the judgment aside. Prior to *Takhar*, there were cases that appeared to question whether Aikens LJ had set too high a test – see *Hamilton v Al Fayed* [2000] EWCA Civ 3012 at [34] (*Hamilton*) and *Salekipour v Parmar* [2017] EWCA Civ 2141 at [93]. But since *Takhar*, two first instance Judges have said that they are not different tests, but two ways of expressing the same test – see *Takhar v Gracefield Developments LLP* [2020] EWHC 2791 (Ch) (*Takhar* 2) at [59] – [60], a decision of Mr Steven Gasztowicz QC, sitting as a deputy Judge of the Chancery Division, in the trial following the Supreme Court's decision in *Takhar*; and *Tinkler* at [22] – [23].
30. I do not need to decide definitively what the test is and am content for the purposes of deciding whether Mr Azima has a real prospect of satisfying the Materiality Condition to accept that there is no real difference in practice between the two tests.

(b) Burden of proof

31. That leads to another issue between the parties as to the burden of proof. Mr Plewman KC submitted that while the burden is on Mr Azima to prove the Fraud Condition, the burden would shift to RAKIA to show that the Materiality Condition was not satisfied. For that surprising proposition, he relies on two matrimonial cases: the Supreme Court decision in *Sharland v Sharland* [2015] UKSC 60 at [33] (*Sharland*); and *C v O* [2021] EWFC 86, a decision of Mostyn J. Mr White KC submitted that these were concerned with special rules relating to non-disclosure in matrimonial ancillary proceedings and have no application to this sort of case. He also pointed out that Lord Hodge, Lord Sumption and Lord Briggs had all sat in both *Sharland* and *Takhar*, but the former was not cited or referred to in the latter. And in *Terry v BCS Corporate Acceptances Limited and ors* [2018] EWCA Civ 2422 at [77], Hamblen LJ (as he then was) said that *Sharland* was confined to matrimonial proceedings, and did not affect "ordinary civil proceedings".
32. Mr White KC also referred to other authorities which indicated that the burden of proving both Conditions was on the party seeking to set aside the judgment. Those cases were: *Hamilton* at [122]; *Dale v Banga* [2021] EWCA Civ 240 at [42] (*Dale v Banga*); and *Park v CNH Industrial Capital Europe Limited* [2021] EWCA Civ 1766 at [3].
33. In my view, the burden is on Mr Azima to establish both Conditions. It does not make sense to me that the burden should shift after the Fraud Condition is proved, particularly as the authorities emphasise how stringent the conditions must be in relation to this cause of action because of the tension between the fraud and finality principles. I therefore reject Mr Plewman KC's submission that RAKIA's failure to establish that the Materiality Condition is not satisfied means that Mr Azima necessarily succeeds without further argument. Mr Azima must demonstrate that he has a real prospect of establishing both Conditions, and I deal with the respective arguments on the facts below.

(c) Where fraud was alleged at the original trial and on appeal

34. *Takhar* was a case where the allegation of fraud, that the defendants had forged the claimant's signature on a document, had not been raised at the original trial. The Supreme Court held that in those circumstances there was no requirement to show that the evidence of fraud could not, with reasonable diligence, have been obtained for the trial. Lord Kerr JSC and Lord Sumption considered *obiter* whether the position would be different had there been an allegation of fraud made at the trial. Lord Kerr JSC said at [55] that there were two qualifications to the general conclusion:

"Where fraud has been raised at the original trial and new evidence as to the existence of the fraud is prayed in aid to advance a case for setting aside the judgment, it seems to me that it can be argued that the court having to deal with that application should have a discretion as to whether to entertain the application. Since that question does not arise in the present appeal, I do not express any final view on it. The second relates to the possibility that, in some

circumstances, a deliberate decision may have been taken not to investigate the possibility of fraud in advance of the first trial, even if that had been suspected. If that could be established, again, I believe that a discretion whether to allow an application to set aside the judgment would be appropriate but, once more, I express no final view on the question."

Lord Sumption at [66] was of a similar view:

"I would leave open the question whether the position as I have summarised it is any different where the fraud was raised in the earlier proceedings but unsuccessfully. My provisional view is that the position is the same, for the same reasons. If decisive new evidence is deployed to establish the fraud, an action to set aside the judgment will lie irrespective of whether it could reasonably have been deployed on the earlier occasion unless a deliberate decision was then taken not to investigate or rely on the material."

35. In this case, Mr Azima was alleging fraud against RAKIA as part of his claim that RAKIA was responsible for the hacking of his data and that its witnesses put forward a false story to cover up what it had actually done. There is no question of any deliberate decision not to investigate. Mr Azima relies on the extensive further evidence that he has now obtained to prove both RAKIA's responsibility for the hacking but also that it perpetrated, as Mr Plewman KC put it, "*a massive fraud on the court*". It appears that there is a discretion, in those circumstances, as to whether he should be allowed to proceed with such a case. To a very great extent, that will depend on the proper interpretation as to the findings in the First Judgment and the CA Judgment and whether it would be an abuse of process to run what the Additional Defendants say is essentially the same case that Mr Azima has run before and which has been decided against him.

THE FIRST JUDGMENT

36. It is therefore important to turn to the First Judgment and then the CA Judgment. (Paragraph references in square brackets are, unless the context otherwise requires, to the First Judgment in this section and the CA Judgment in the next.)
37. As indicated above, RAKIA pursued claims in fraudulent misrepresentation and conspiracy against Mr Azima. There were two representations that RAKIA said it relied upon in entering into the Settlement Agreement:
- (1) A representation by Mr Azima that HeavyLift had invested certain sums into a joint venture with RAK Airways (the **Investment Representation**); and
 - (2) A representation and warranty (as set out in clause 3.2 of the Settlement Agreement) that he had at all times acted in good faith and with the utmost professional integrity towards RAKIA, RAK Airways and other RAK government entities (the **Good Faith Representation**).
38. The unlawful means conspiracy claim was in connection with the intended sale of the Hotel in 2011-2012 and the payments of commission to Mr Azima for introducing the buyers of it. RAKIA's case was that Mr Azima did not introduce the buyers and that the payments were made pursuant to a sham referral agreement.
39. Mr Azima defended the claims on their merits but also by arguing, as per his hacking counterclaim, that the claims "*should be struck out or dismissed on the ground that, in bringing the claims, RAKIA is relying on confidential emails that RAKIA obtained through its unlawful hacking of his email accounts*": [10].
40. At the start of the First Judgment, the deputy Judge dealt with the background facts and the general credibility of the witnesses that gave evidence. In relation to RAKIA's evidence, his findings were broadly as follows:

(1) The Ruler of RAK, Sheikh Saud bin Saqr Al Qasimi (**Ruler**) provided a witness statement but did not attend for cross-examination. The deputy Judge said that he would not "*attach significant weight*" to the Ruler's witness statement as it was not tested by cross-examination [59], but that his evidence did carry some "*limited weight*": [174].

(2) Mr Buchanan was "*a generally reliable witness*": [61].

(3) Mr Gerrard was not a dishonest witness: [63].

(4) Mr Page was an "*unsatisfactory and unreliable witness*": [64].

(5) Mr del Rosso's evidence was "*uncontroversial*": [69].

(6) RAKIA had not engaged in deliberate document destruction: [77].

41. The deputy Judge dealt with the claims in relation to the Investment Representation in [78] to [159]:

(1) The deputy Judge held that the Investment Representation was made fraudulently on Mr Azima's behalf and with Mr Azima's knowledge. In reaching that conclusion, the Judge made a series of findings of dishonesty or other misconduct on the part of Mr Azima: see eg [71], [93], [96], [97], [105], [112], [113], [117]-[120], [128] and [138]-[145].

(2) The deputy Judge concluded that RAKIA had relied on the Investment Representation in deciding to enter into the Settlement Agreement, relying on the principle that "*[i]t is not necessary to prove that the misrepresentation was the sole or even predominant cause of the decision to enter the contract but it is necessary to show that misrepresentation contributed to the decision to contract*": [146]-[154].

42. As to the Good Faith Representation [160]-[246], the deputy Judge found that Mr Azima had engaged in several forms of wrongdoing in his dealings with RAKIA, as follows:

(1) Mr Azima falsely represented that he had introduced the potential purchasers of the Hotel to RAK Georgia. The main basis for the finding that he had not effected the introduction was a memorandum dated 1 March 2016 (the **Adams Memorandum**), written over four years after the events in question, in which Mr Ray Adams (Mr Azima's right hand man and witness) had recounted a trip he and Mr Azima had made to Georgia in 2011: "*We were informed that a group of businessmen from Dubai were already negotiating the purchase of the SMP [the Hotel] and were introduced to them.*"

(2) Mr Azima created a false referral agreement between Mr Azima and RAKIA which purportedly entitled Mr Azima to 5% of the gross sale price of the Hotel plus 50% of any amount in excess of \$50 million but which was in fact a sham intended to conceal misappropriation of funds by Mr Azima.

(3) Mr Azima paid a bribe of \$500,000 to Dr Khater Massaad, RAKIA's former Chief Executive Officer, on 18 January 2012, the day on which Mr Azima received a payment of \$1,162,500 from RAKIA to which he claimed to be entitled under the referral agreement.

(4) If (contrary to the deputy Judge's conclusion) the referral agreement was not a sham, Mr Azima wrongfully failed to disclose to RAKIA his intended interest in the Hotel (in breach of the referral agreement).

(5) Mr Azima oversaw the commissioning of and payment for a "*Security Assessment*" report, which included a recommendation by which the RAK Government and associated parties could be deceptively lured into entering transactions with serious criminals and deliberately exposed to "*Scams, fraud and deceptive partnerships*".

(6) In the context of a proposed joint venture between RAKIA and Global Defence Services, a corporation of which Mr Azima was a major shareholder and director, Mr Azima made a false representation to RAKIA as to the value of the aircraft that would be acquired by the joint venture.

43. In light of these findings of misconduct by Mr Azima, the deputy Judge held that Mr Azima had not acted in good faith towards RAKIA and the Good Faith Representation was therefore found to be false. The deputy Judge held that RAKIA had relied on these misrepresentations, with his reasoning at [244] being that:

"The evidence establishes that both Mr Buchanan and the Ruler relied on the Good Faith Representation. Whilst the Ruler and Mr Buchanan may have harboured suspicions about Mr Azima, it does not follow that they did not rely on the Good Faith Representation. The fact that a representee harboured suspicions regarding the honesty of a representor does not negate inducement (see *Zurich Insurance Co plc v Hayward* [2017] AC 142 at [18]-[20] (Lord Clarke) and [67]-[71] (Lord Toulson))."

44. As to the conspiracy claim, the deputy Judge considered that it was reasonably to be inferred from (a) the receipt by Dr Massaad of a bribe from the illicit payments purportedly made under the sham referral agreement and (b) the involvement of Mr Karam Al Sadeq (the former deputy CEO of RAKIA) in the retrospective drafting of the referral agreement, that Mr Azima had agreed at least with Dr Massaad and probably with Mr Al Sadeq that the illicit payments would be made. Mr Azima was therefore liable to RAKIA in unlawful means conspiracy: [247]-[250].

45. In relation to Mr Azima's hacking claim, the deputy Judge concluded that Mr Azima had not proved on the balance of probabilities that RAKIA was responsible for the hacking of his data. Even though he did not accept Mr Page's evidence as to how he allegedly discovered the hacked material, he held that Mr Gerrard and Mr Buchanan did not know about it until it was published online. He went on: "*More generally, I was not satisfied that there was sufficiently cogent evidence to establish a conspiracy between the RAKIA witnesses to advance a false case in these proceedings.*" Mr Azima says that he now has much more evidence to show this, including an admission to that effect by Mr Page.

46. The deputy Judge, at the end of the First Judgment at [384], explained what he might have done had he found that RAKIA was responsible for the hacking:

"If I had found that RAKIA had hacked Mr Azima's emails, I would not necessarily have excluded the illicitly obtained evidence as, without it, RAKIA would have been unable to prove its claims and Mr Azima would have been left with the benefit of his seriously fraudulent conduct. If, however, I had found that, as alleged by Mr Azima, not only had RAKIA hacked Mr Azima's emails and used them as the evidential basis of this case, but also that its witnesses had conspired to put forward a fabricated case concerning RAKIA's lack of involvement in the hacking, there would have been strong grounds to strike the proceedings out as an abuse of process, as envisaged in *Summers v Fairclough Homes Ltd.*"

47. In the CA Judgment at [49], the first sentence in the quote above was approved. However the second sentence was not referred to and it is relied upon by Mr Azima as showing the consequence of putting forward a fabricated case to the Court, which is what he says RAKIA did.

THE CA JUDGMENT

(a) Grounds of Appeal

48. Mr Azima was granted permission to appeal by Arnold LJ. Grounds 1 to 4 of his appeal concerned the deputy Judge's findings as to RAKIA's responsibility for the hacking. Then Ground 5 was a main plank of the appeal. It was in the following terms:

"Ground Five: the Judge should have gone on to find that RAKIA was responsible for the hacking and that RAKIA's claims fell to be struck out as an abuse of the process and/or the evidence obtained through hacking excluded as inadmissible."

Mr Plewman KC maintained that this Ground was put forward on the somewhat limited bases of exclusion of evidence or striking out after trial in reliance on the authorities of *Jones v University of Warwick* [2003] EWCA Civ 151 and *Summers v Fairclough Homes Limited* [2012] UKSC 26, both of which were discussed in the CA Judgment. He submitted that the way Mr Azima puts his case now is that there was a far more pervasive fraud in relation to the original trial such that the First Judgment should be set aside.

49. Mr Azima also sought to adduce some new evidence in the Court of Appeal in support of his claim that RAKIA was responsible for the hacking. This was:

(1) Evidence of various alleged "*phishing*" emails sent to Mr Azima and those associated with him.

(2) Evidence obtained by a security consultant, Mr Jonas Rey, who had investigated the hacking for Mr Azima and had discovered the involvement of an Indian company called CyberRoot Risk Advisory Private Limited (**CyberRoot**) which had been paid \$1 million by Vital Management Services Inc, Mr Del Rosso's company. Mr Del Rosso had been a witness for RAKIA at the original trial but had not mentioned CyberRoot. Mr Rey had spoken to a former employee of CyberRoot, Mr Vikash Pandey, who admitted that CyberRoot had hacked Mr Azima's data from June/July 2015, on the instructions of Mr Del Rosso and using infrastructure made available by another Indian company, BellTrox Info Tech Services (**BellTrox**).

50. This new evidence was the subject matter of Grounds 6(A) and (B) as follows:

"Ground Six (A): In view of new evidence as to numerous phishing emails sent to Mr Azima and other persons associated with him and RAK-related matters, considered together with the other factors pointing to RAKIA's responsibility, RAKIA should be found responsible for the hacking and the consequences set out in Grounds Five and Six should follow.

Ground Six (B): In view of new evidence as to the activities of Mr Del Rosso and Vital Management Services Inc, and Cyber Root Risk Advisory Private Limited, considered together with the other factors pointing to RAKIA's responsibility, RAKIA should be found responsible for the hacking and the consequences set out in Grounds Five and Six should follow."

51. Mr Azima was also appealing the deputy Judge's findings on RAKIA's claim and sought to adduce new evidence in such respect in the form of a witness statement from Mr Pourya Nayebi on the issue of whether Mr Azima had introduced Mr Nayebi (and the other two potential purchasers) to the Hotel transaction. He added a new Ground 8(A) but the Court of Appeal did not admit this evidence. Mr Azima still persisted in his appeal against the findings in relation to RAKIA's claim, in particular as to whether RAKIA relied on the Investment and Good Faith Representations.

52. It is clear from the skeleton arguments filed in support of his appeal that, if the new evidence in relation to hacking was admitted, Mr Azima would be asking the Court of Appeal to do one of two things: either to accept that RAKIA was responsible for the hacking and to uphold the appeal including in relation to RAKIA's claims; or to remit the hacking issue to be retried with the consequential impact on RAKIA's claims, if RAKIA was found to be responsible for the hacking, to be left to the Judge hearing the remitted claim. In other words, Mr Azima wanted his hacking claim to be upheld and RAKIA's claims against him dismissed.

(b) Mr Azima's oral submissions before the Court of Appeal

53. The Additional Defendants all focused much attention on how Mr Azima's appeal was put orally by Mr Tim Lord KC on his behalf. There is no doubt that the case was put very high, with Mr Lord KC repeatedly alleging that RAKIA and its witnesses had fraudulently deceived the Court in their evidence at trial, and that the fraud practised by them, which he characterised as "*massive deception that it sought to practise on the court*", was material to the findings of the Judge in upholding RAKIA's claims. Mr Lord KC alleged that "*the connection between the hacked material and the case advanced means that the whole claim is contaminated*", and that dishonesty on the part of RAKIA "*contaminates the whole trial process and therefore it contaminates the findings in this case in favour of RAKIA on its claims*".
54. Mr Lord KC referred a number of times to Mr Azima being entitled, by way of an alternative to the appeal, to bring proceedings to set aside the entirety of the First Judgment (including RAKIA's claims) on the ground of fraud. For example, he submitted:

"Given the nature of the further evidence that Mr Azima has now managed to find, he would be entitled to bring fresh proceedings in the High Court to set aside the judgment of Deputy Judge Lenon on the basis that RAKIA had procured that judgment by fraud, and there could be no answer really from RAKIA that it was an abuse, so there could be fresh proceedings to set aside the judgment. And not just the hacking judgment, but the judgment, because that would be the order that would be set aside. [...] what Mr Azima has done, quite properly we say and as the court might well expect him to do, is to bring this further evidence before this court on this appeal so that this court is able to consider whether this evidence should be considered by way of a remission to the court within the existing proceedings that are on appeal, rather than having the inefficient and slow process of starting fresh process and that, far from Mr Azima being liable to be criticised for what he's done, as RAKIA do, he's actually done the right thing.

Mr Azima had options here. He could have simply issued fresh proceedings, but, quite properly, given this pending appeal, he has deployed this further material on this appeal"

55. The context for these submissions was that the appeal had been launched before the new evidence had been obtained. When it had been obtained the issue was then whether it should be deployed in the existing appeal or whether fresh proceedings should be started to attempt to set aside the original judgment for fraud. Before the case of *Noble v Owens* [2010] EWCA Civ 224, it was thought that such an allegation should not be raised on appeal and fresh proceedings were required (see the commentary at CPR 52.21.3 which refers to *Flower v Lloyd* (1877) 6 ChD 287 and *Jonesco v Beard* [1930] AC 298). From 2010, the practice changed as explained by Asplin LJ in *Dale v Banga* which was delivered a week before the hearing of Mr Azima's appeal.
56. There was a discussion as to whether, if the new evidence was admitted, the fraud allegation should be remitted to be tried within the same proceedings or whether Mr Azima should pursue the allegation in a new claim. Mr Lord KC firmly favoured the remittal and this was relied on strongly by the Additional Defendants who submitted that Mr Azima had thereby made an election and decided not to pursue a fresh claim to set aside the First Judgment on the grounds of fraud. However, it must be understood that Mr Lord KC's submissions were all predicated on the whole claim, including RAKIA's claims, being remitted for a retrial, or at least it being open to the retrial Judge to set aside RAKIA's claims if the fraud was proved. His submissions were not directed at the situation where only the hacking counterclaim would be remitted together with a direction that RAKIA's claims could not, under any circumstances, be disturbed.

(c) The CA Judgment

57. It is important to look at the CA Judgment in some detail.

58. Mr Lord KC's position, as outlined in the paragraph above, was recorded at the start of the CA Judgment. He was asking the Court of Appeal to find, as a matter of fact, based on the new evidence, that RAKIA had hacked Mr Azima's email accounts, with the consequence that *"the action should be struck out as an abuse of process"* by the Court of Appeal. In the alternative, Mr Azima was asking the Court of Appeal for a remittal of the whole proceedings:

"In the alternative it is argued that the issue whether RAKIA was responsible for the hacking should be remitted for a retrial; and since the judge's decision that Mr Azima had not proved his hacking allegation was fundamental to at least some of his conclusions on RAKIA's substantive claims, they, too, should be remitted for a retrial." [8]

59. After setting out the factual background and a summary of the deputy Judge's findings, the Court of Appeal explained the approach it was going to adopt to considering the issues on the appeal. At [39], it explained that it was taking the issues in a different order to that in which they were advanced. The first issue was: *"whether, if RAKIA was responsible for the hacking, the evidence obtained through hacking ought to have been excluded; or its claims should have been (or should now be) struck out."* So before even considering the new evidence, the Court of Appeal was deciding whether it could impact on RAKIA's claims.

60. In order to do so, it had to make certain assumptions adverse to RAKIA as to what that evidence might show. The Additional Defendants rely heavily on those assumptions and the conclusions of the CA Judgment in this respect. At [40], the CA Judgment stated:

"We will assume, for present purposes, (a) that RAKIA's case would have failed but for the existence of documents obtained as a result of the unlawful hacking of Mr Azima's computer; (b) that RAKIA was responsible for that unlawful hacking; and (c) that at least some of RAKIA's witnesses gave dishonest evidence about how RAKIA came into possession of the hacked material" (emphasis added).

61. The CA Judgment then discussed the two strands of Mr Azima's argument on this aspect, namely: whether the evidence should have been excluded (based on *Jones v University of Warwick*); or whether RAKIA's claims should have been struck out (based on *Summers v Fairclough Homes Limited*). The Court of Appeal held that, even if the factual assumptions in [40] were established, it would not be appropriate to exclude the unlawfully obtained evidence or to strike out RAKIA's claims. It said that *"any unlawful conduct by RAKIA in obtaining the emails was not central to its underlying claims against Mr Azima"*: [60]. In [61] it only referred to Mr Page's and Mr Halabi's evidence and said that even if they had *"told lies, they were collateral or lacked centrality in this sense: because they did not go to the merits of RAKIA's underlying claims."* Mr Plewman KC submitted that this showed the limited nature of the assumptions made by the Court of Appeal and it was not considering a wider conspiracy, involving Mr Buchanan and Mr Gerrard, both of whom did give evidence on the underlying claims.

62. The CA Judgment referred to the strong policy reasons for not striking out RAKIA's claims in these circumstances. At [62], the CA Judgment stated:

"Three other points are worthy of note. First, as we have said, the hacked materials ought to have been disclosed by Mr Azima anyway (except to the extent that they were legitimately covered by legal professional privilege). Second, to strike out RAKIA's claim would leave Mr Azima with the benefit of his fraud. That element of public policy in civil cases is at least as strong, if not stronger, than disapproval of the means by which relevant evidence is gathered. Third, there are other ways in which the court may express its disapproval of the conduct of a party found to have procured relevant evidence by unlawful means: notably by penalties in costs or, perhaps, the refusal of interest on damages awarded."

And at [63] it concluded:

"In our judgment, even if the judge had found that RAKIA had been involved in the hacking of Mr Azima's email accounts, it would have been wholly disproportionate to have struck out its claim, thereby leaving Mr Azima with the benefit of his frauds."

63. The CA Judgment went on to reject Mr Azima's challenges to the deputy Judge's reasoning in upholding RAKIA's claims, including disallowing the admission of the proposed new evidence from Mr Nayebi. It concluded that *"the attacks on the judge's findings of fact in relation to RAKIA's claims fail; and that even if RAKIA was responsible for the hacking those claims should not be struck out or dismissed"*: [122]. This was reiterated at [128] where the Court of Appeal stated that *"irrespective of the outcome of the counter claim the judgment in RAKIA's favour on its claims must stand"*.
64. By this stage of the CA Judgment, the Court of Appeal had already decided that RAKIA's claims against Mr Azima would stand whatever the outcome on the hacking allegations. It then went on to consider those allegations and what should happen to them.
65. In [130] to [134], the Court of Appeal looked at the proposed new evidence and decided that it could not resolve the factual dispute and the hacking counterclaim would need to be retried. It therefore admitted the fresh evidence but remitted the counterclaim to be retried by a different Judge.
66. Before doing so, the CA Judgment considered that there were *"two alternatives"* open to a litigant who alleges that a *"judgment was procured by fraud"*, namely that *"the litigant alleging fraud may bring a separate action to set aside the judgment"* or *"the court may direct a trial of the fraud issue within the existing action"*: [135]. The Court of Appeal then went on to consider *Takhar and Dale v Banga* in the context of deciding between the alternative routes for determining whether RAKIA was responsible for the hacking.
67. I have to say that I am a little confused about the reference in [135] to a judgment that *"was procured by fraud"* and the possibility of a fresh action to set it aside. The Court of Appeal had already decided that the judgment in favour of RAKIA on its claims against Mr Azima would not be set aside under any circumstances and whatever the outcome of the hacking counterclaim. So it could not be that judgment that Mr Azima might be allowed to apply to set aside. Mr Plewman KC submitted that it was the dismissal of the counterclaim that the Court of Appeal contemplated being set aside on the grounds of fraud. But that strikes me as a very odd way of going about things and not a sensible alternative to a retrial of the counterclaim. Mr Masefield KC submitted that this was a reference to the judgment on RAKIA's claims but that would be inconsistent with the Court of Appeal having already found that that judgment could not be set aside.
68. The CA Judgment continued to consider Mr Lord KC's primary submission that the Court of Appeal should itself decide that RAKIA was responsible for the hacking. At [141], the Court of Appeal declined to do so and then considered how that issue should be dealt with.
69. Then the alternatives referred to at [135] were repeated at [142] again suggesting that there could either be a remittal of *"the issue of fraud"* or Mr Azima could *"begin a fresh action"*. The Court of Appeal said that Mr Lord KC argued for remittal; whereas Mr Hugh Tomlinson KC for RAKIA argued for a fresh action. However, from what I have seen of the argument, Mr Lord KC was arguing for a remittal of the whole matter including RAKIA's claims and he was not asked what he would prefer if it was only the hacking counterclaim that was going to be remitted and RAKIA's judgment on its claims would remain undisturbed.
70. The Court of Appeal was only *"narrowly persuaded"* to remit the counterclaim rather than leaving Mr Azima to begin a fresh action. It recognised the difficulty of remitting back to the deputy Judge, so specified that it should be to another Judge. It then added: *"[r]emission in the current action also has the benefit that RAKIA's judgment against Mr Azima on its own claims will stay in place, irrespective of the outcome of the counterclaim"*: [145], which suggests that, if this was a benefit of remittal, a fresh action could have interfered with RAKIA's judgment against Mr Azima.

71. Finally, in [146] the Court of Appeal specified the scope of the remitted matters: *"that neither the parties nor the judge who hears the remitted issues will be bound by any of the findings of fact made by the judge on the hacking claim. But his findings of fact on RAKIA's substantive claims stand."*

72. The CA Order consequential on the CA Judgment, relevantly provided:

"2. The appeal on ground 6 is allowed and paragraph 8 of the High Court Order is set aside.

3. The Appellant's counterclaim is remitted to the Chancery Division of the High Court to be tried by a judge nominated by the Chancellor of the High Court.

4. In respect of ground 5, it is declared that even if it is established on the counterclaim that the Respondent was responsible for the hacking and dissemination of the Appellant's data:

a. the evidence obtained as a result of the hacking should not be excluded; and

b. the Respondent's claims against the Appellant should not be struck out.

5. Save as set out herein:

a. No further order is made as to Grounds 1-4;

b. Ground 5 is otherwise dismissed;

c. No further order is made as to Grounds 6A and 6B.

6. The appeal under grounds 7, 8 and 9 is dismissed.[...]

...

12. In the event that the Respondent succeeds in his counterclaim:

a. paragraph 1(b) of the High Court Order is set aside and the question of any interest on the damages awarded to the Respondent shall be in the discretion of the Nominated Judge...

b. paragraphs 3-7 of the High Court Order are set aside and the question of the costs of the Respondent's claim against the Appellant (including any interest on costs and any interim payment) shall be in the discretion of the Nominated Judge..." (emphasis added)

APPLICATION TO THE SUPREME COURT

73. Mr Azima filed his application for permission to appeal to the Supreme Court on 8 April 2021. Under the proposed Grounds of Appeal, Mr Azima stated that the *"central focus"* of an appeal to the Supreme Court would be that *"...despite remitting the hacking issue for retrial, the CA pre-emptively determined that even if RAKIA was responsible for the hacking and had systematically deceived the court, the possible remedies were confined to the counterclaim and a re-assessment of interest and costs"* and that *"regardless of how serious RAKIA's wrongdoing and deceit may be shown to have been: [...] (3) RAKIA's wrongdoing will not impact its claims, even though they depended in key respects on the credibility of its account"*. Accordingly the issues in the prospective appeal included:

"(1) Whether the remedy of striking out a claim for abuse of process or excluding evidence relied on by the Claimant, can be or should have been excluded before that serious wrongdoing and dishonesty have been fully investigated"; and

(4) Whether not only the counterclaim but also some or all of RAKIA's claims and all of the defences to them ought to have been remitted".

74. This was therefore a point of law that Mr Azima said the Court of Appeal had got wrong. It should not have provided for such a narrow remission of the counterclaim. Mr Azima said that the Court of Appeal should not have rejected the remedy of strike out for abuse of process before the extent of the findings on the retrial were known. He said:

"54. ...if Mr Azima had only obtained the new evidence after the appeal, he could have applied to have the judgment set aside as procured by fraud. If RAKIA's case rested upon a fabricated and dishonest foundation, that relief would have been appropriate –*Takhar v Gracefield Developments Ltd* [2019] 2 WLR 984, at [46]. Mr Azima properly raised the new evidence on appeal once it became available. It is wrong in principle for the CA's decision to exclude that possibility before investigating the dishonesty."

75. Before the Supreme Court made its decision, Mr Azima filed two applications, on 10 January 2022 and 3 February 2022, for permission to rely on fresh evidence, in the form of affidavits from Mr Page sworn on 7 January 2022 and from Mr Majdi Halabi sworn on 2 February 2022. Both Mr Page and Mr Halabi had given evidence at the original trial about the alleged innocent discovery of the hacked material. In their new affidavits they admitted that the evidence they had given had been false and had been deliberately concocted together with Mr Buchanan, Mr Gerrard and another partner at Dechert, Mr David Hughes. Mr Page also admitted that RAKIA was responsible for the hacking of Mr Azima's data. In the application, Mr Azima said that this evidence showed that RAKIA had provided false testimony at the trial and had procured the judgment by fraud. It went on to say that: *"It should also be noted that where new evidence shows that an earlier judgment had been obtained by fraud, this would provide a basis for a fresh action to set aside that judgment, or the appellate court may direct that trial of the fraud issue is remitted"*.

76. Despite the new evidence and the points raised in the application, the Supreme Court Order dated 28 April 2022 (Lord Reed, Lord Sales and Lord Stephens JJSC) refused permission to appeal on the basis that the application did not raise an arguable point of law.

77. Mr Plewman KC said that not much could be read into the Supreme Court's refusal of permission and I am inclined to agree. There are no reasons given. All we do know is that the Supreme Court decided that there was no arguable point of law. That must be a reference to the main ground of appeal as to the appropriateness of the CA Order remitting the counterclaim but not allowing any interference with RAKIA's judgment on its claims. The extent to which the Supreme Court took into account the new evidence is impossible to tell but it was clearly not prepared to countenance any appeal on factual issues.

THE NEW EVIDENCE

78. Mr Azima had obtained certain new evidence as to RAKIA's responsibility for the hacking after the original trial and this was admitted into evidence by the Court of Appeal. This was the phishing emails and the evidence from Mr Rey. After the CA Judgment and several months after the application for permission to appeal to the Supreme Court had been made, Mr Azima had the affidavits of Mr Page and Mr Halabi in which they admitted that their evidence at the trial had been dishonestly fabricated and alleged that this had been orchestrated by Mr Gerrard, Mr Buchanan and Mr Hughes.

79. During the course of a hearing before me on 15 and 17 March 2022, I asked whether Mr Page had ever raised invoices for his work to RAKIA. After instructions, Mr Tomlinson KC said that *"there are no invoices from Mr Page to RAKIA. The documents have been previously searched and none have been found"*. However, following inquiries made of Mr Page's solicitors, a whole series of invoices from a company of Mr Page's called PGME JLT addressed to RAKIA between February 2015 and February 2019 have been disclosed. The invoices had a false narrative of the work done – they stated that the work was *"conducting feasibility study to identify potential to provide management services in the African Subcontinent establishing Freezones"*. Mr Azima says that this was to mask the real activity that was taking place which was the illegal hacking of Mr Azima's data. RAKIA has not disputed that these invoices were received and paid; nor has it denied that they contained a false narrative. The invoices were not disclosed during the original trial and they should have been.

80. The work that Mr Page principally did for RAKIA in this respect was to compile what were called Project Update Reports for submission to the Ruler, Mr Buchanan and Mr Gerrard (on occasion). At the trial, RAKIA disclosed a heavily redacted Project Update Report from March 2015. Mr Azima asked for the redactions to be removed but this was resisted on the basis that the redactions concerned irrelevant and confidential material. This was referred to in the First Judgment and the deputy Judge also said that Mr Page and Mr Buchanan had given evidence that all the other Project Update Reports had been routinely destroyed pursuant to a "*protocol*". The redacted copy was still the only Project Update Report before the Court of Appeal.
81. Following a further application by Mr Azima in May 2022, Dechert disclosed the full unredacted March Project Update Report. Mr Azima says that it should never have been redacted in the first place because there was relevant material redacted including in particular information about Dr Massaad and his company Star Industrial Holdings Limited. He has never received a response from RAKIA or its former solicitors, Stewarts, as to why the redactions were made.
82. In the course of June 2022, Mr Azima obtained very many more Project Update Reports and associated materials. These were provided by Mr Page's assistant who had saved some of the Reports. In order to ensure that third-party privilege was not breached, the Reports were provided to an independent barrister to review prior to their disclosure to Mr Azima. Having followed that process, there are now a large number of Reports from 2015 and 2016. They are said to relate to "*Project Beech*" which seems to be the code name for RAKIA's investigations into Dr Massaad and his associates including Mr Azima.
83. Mr Azima says that a review of the Project Update Reports shows that RAKIA had access to the hacked material, including privileged and confidential emails, from well before it was published online and before the Settlement Agreement was entered into. This shows conclusively, he says, that RAKIA's case on hacking has been thoroughly dishonest throughout and that the deputy Judge and the Court of Appeal have been seriously deceived. It was the discovery and review of the Project Update Reports that led to the application for permission to make the additional counterclaim on 24 June 2022. Mr Azima says that they were deliberately withheld from the original trial in order to allow the false and dishonest evidence to be given by RAKIA's witnesses.
84. Mr Plewman KC took me through some of the Project Update Reports. They contained highly confidential financial and banking information about Mr Azima and his wife and emails sent by or to Mr Azima that could only have been illegally obtained. Mr Masefield KC submitted that Mr Page had referred in his affidavit to the fact that the Project Update Reports had contained extracts from what he assumed had been hacked material and so the actual provision of the Reports themselves does not actually shift the dial very much. However, it is striking to see Mr Page's general allegations in his affidavit confirmed in contemporaneous documentary form, which may be difficult for RAKIA to dispute. It would potentially be easier to dismiss Mr Page's evidence as lacking credibility if it was not supported by the actual underlying documents.
85. In reliance on the recently available Project Update Reports Mr Azima has pleaded them fully in the draft RRRACC, in particular in Schedule B which sets out the alleged contradictions between RAKIA's case at trial and what the new evidence shows. These allegations were summarised by Mr Plewman KC as RAKIA, through the actions of the Ruler, Mr Buchanan and Mr Gerrard, being shown to have:
- (1) procured the hacking of Mr Azima's documents as part of its investigations;
 - (2) arranged for the materials stolen from Mr Azima to be placed online in order to provide an innocent explanation for how it came across the data;
 - (3) created a false documentary trail to support the "*innocent discovery*" story;
 - (4) dishonestly destroyed, withheld and/or failed to identify the documentary evidence revealing the scale of RAKIA's unlawful investigations of Mr Azima;

(5) provided false witness evidence through the Ruler's witness statement;

(6) suborned the perjurious testimony of Mr Page, Mr Halabi, Mr Buchanan and Mr Gerrard in order to conceal the hacking, support the innocent discovery story, and conceal the fraud from the Court; and

(7) withheld disclosure concerning the Hotel transaction, and dishonestly concealed (in its evidence and otherwise) information regarding that transaction and RAKIA's knowledge of it.

86. I have to assume for the purposes of this application that Mr Azima has at least a real prospect of establishing this on the facts. That would clearly constitute "conscious and deliberate dishonesty" sufficient to satisfy the Fraud Condition and the Additional Defendants do not suggest otherwise.

87. However I do now turn to the reasons why the Additional Defendants say that permission should be refused.

JURISDICTION

88. The Additional Defendants submitted that I do not have jurisdiction to allow the additional counterclaim to be brought. They say that the terms of the CA Order limit my jurisdiction to the matters expressly remitted to be tried and I have no power to extend my own authority to something which the Court of Appeal held should not be disturbed.

89. Mr Masefield KC referred to the CA Judgment's clear findings that the judgment in RAKIA's favour on its claims against Mr Azima must stand regardless of the outcome of the retrial of the hacking counterclaim and that my role as the assigned Judge is limited to the specific issues in relation to hacking that were remitted ([128], [145], [146] of CA Judgment). The CA Order declared in paragraph 4 that the outcome of the remitted counterclaim should not impact on RAKIA's claims against Mr Azima and his appeals against those claims were dismissed (paragraphs 7 to 9 of the CA Order). He submitted that the only way for Mr Azima to challenge this would be to apply to the Court of Appeal to reopen the CA Order under CPR 52.30.

90. Mr Masefield KC cited *Zuckerman on Civil Procedure: Principles of Practice* (4th Ed.) at [25.267]:

"The lower court is functus officio once it has delivered its [sic] decision. Consequently, it has no power to reconsider its decision unless ordered to do so by the appeal court. Care must therefore be taken when making a referral to identify the matters that the lower court may or should reconsider."

91. Mr White KC made some brief submissions on jurisdiction and referred to an arbitration case in which the Court of Appeal had remitted one issue back to the arbitrators and Steyn J (as he then was) held that the arbitrators could only consider the one issue that had been remitted to them and nothing else: *Interbulk Limited v Aiden Shipping Co Limited (The Vimeira)* (No 3) [1986] 2 Lloyd's Rep 75. Mr White KC said that this was an *a fortiori* case because the Court of Appeal specifically directed that the judgment obtained by RAKIA against Mr Azima should not be remitted or otherwise interfered with.

92. Mr Plewman KC responded to these points principally on the basis that the High Court's jurisdiction to hear applications to set aside judgments or orders procured by fraud cannot be ousted. The High Court has an inherent jurisdiction to hear such applications – see *Salekipour* at [70] – and Mr Azima could have started separate proceedings in the High Court which could then have been consolidated with the remitted counterclaim. Therefore the scope of the matters remitted by the Court of Appeal cannot deprive the High Court of jurisdiction to hear such a claim.

93. Mr Masefield KC submitted that this was not a good answer to the lack of jurisdiction for two reasons: (a) Mr Azima has not issued a fresh claim to set aside the judgment and he cannot rely on a procedure that he has not adopted; and (b) in any event, Mr Azima is not free now to issue a fresh claim because he chose

not to pursue that course in the Court of Appeal, arguing strongly for the case to be remitted to the High Court.

94. I do not think that this adequately answers Mr Plewman KC's argument. As I have said above, the test for whether permission should be given must be the same whether the claim is brought by fresh proceedings (where permission may not be required but there may be an application to strike out on the grounds of abuse of process) or within the existing proceedings. And the only reason why Mr Azima might not be able now to pursue a fresh claim is if the Additional Defendants are correct on their abuse of process argument. I consider that the main substantive issue is in relation to abuse of process which I discuss below.
95. If a fresh claim could have been brought, then I do not think I am limited by the CA Order in deciding whether to consolidate it for sound case management reasons with the remitted counterclaim. There are essentially the same factual issues to be determined and it makes sense, from both the parties' and the Court's perspectives, for them to be tried together. I have already allowed the Additional Defendants to be joined to the counterclaim and permitted substantial amendments to the pleadings, which shows that my jurisdiction has not been limited to the counterclaim remitted by the Court of Appeal. Mr Masefield KC said that the Court of Appeal anticipated that there would be amendments to the pleadings and did not consider any additional parties (so it did not expressly rule that out). However the Court of Appeal did expressly rule out any interference in RAKIA's judgment against Mr Azima which it had upheld.
96. I do not think that the Court of Appeal could have considered that it was removing, in all circumstances, the High Court's jurisdiction to hear an application to set aside the judgment on the grounds of fraud. If the most damning evidence of fraud emerged, say a clear confession by Mr Buchanan that they had all deliberately lied to the Court at the original trial and they knew that the Settlement Agreement was a trap, it would be very odd if the High Court was debarred from hearing an application based on such evidence.
97. As to whether Mr Azima should have used the procedure under CPR 52.30 and applied back to the Court of Appeal, Mr Plewman KC referred to *Flower v Lloyd* and *Jonesco v Beard* (both cited above) as showing that the correct procedure in these circumstances is to start fresh proceedings. This is based more on the fact, which was recognised in the CA Judgment, of the difficulties of an appeal court trying contested issues of fact, particularly where there are allegations of fraud – see also *Jaffray v Society of Lloyd's* [2008] 1 WLR 75 (*Jaffray*).
98. This is further demonstrated by *Kuwait Airways Corp v Iraqi Airways Co (No. 8)* [2001] 1 WLR 429 where the House of Lords dismissed a petition to reopen the appeal and directed the appellant to issue a fresh claim. That fresh claim was heard by David Steel J in *Kuwait Airways Corp v Iraqi Airways Co (No. 11)* [2003] EWHC 31 (Comm) and he set aside the House of Lords' earlier decision and order. So it is clear that if the fraud is established and both Conditions are met, the High Court can set aside orders of the Court of Appeal or Supreme Court.
99. The jurisdiction to reopen appeals under CPR 52.30 is only available in exceptional circumstances, where it is necessary to do so "in order to avoid real injustice" and where "there is no alternative effective remedy". Mr Azima says that he wishes to pursue the more appropriate remedy of applying to set aside the First Judgment and CA Order for fraud and that accordingly there is no jurisdiction in CPR 52.30 to apply to reopen the appeal.
100. Mr Plewman KC referred to the End Note in *R (Wingfield) v Canterbury City Council* [2020] EWCA Civ 1588 (*Wingfield*) which cited *Jaffray* for the proposition that there is doubt as to whether CPR 52.30 is available in cases of fraud which could be used as the basis for a fresh action and so not the only available remedy. Mr White KC however submitted that in [59] and [61(3)] of *Wingfield* the Court of Appeal indicated that the paradigm case for the use of CPR 52.30 was a case of "fraud or bias or where the judge read the wrong papers" and if that is the paradigm case it cannot be ruled out by the availability of alternative relief. But I do not think that the Court of Appeal was there considering whether a separate claim could be brought to set aside the order as having been procured by fraud. There seems to be more of a focus on what the judge may have done to render the outcome an injustice.

101. In my view, there is jurisdiction, in the pure sense, to give Mr Azima permission to bring the additional counterclaim to set aside the First Judgment and CA Order for fraud. The High Court has not been deprived of jurisdiction to hear such a claim and it does constitute an alternative effective remedy so as to rule out an application to the Court of Appeal under CPR 52.30. The main and critical question is whether the bringing of that additional counterclaim would be an abuse of the Court's process.

ABUSE OF PROCESS

(a) Introduction

102. The Additional Defendants submitted that the proposed additional counterclaim would be an abuse of process in that Mr Azima is seeking to re-litigate matters that have already been considered and decided against him by the Court of Appeal and possibly the Supreme Court; alternatively that it would constitute a collateral attack on the CA Judgment. In short, they contend that this would be Mr Azima's second or third bite of the cherry and the finality principle should prevent him from doing so.
103. While it is true to say that the Court is itself concerned to protect its processes from abuse and in particular the wasteful and disproportionate use of its resources, the finality principle is primarily focused on a party not being vexed endlessly by the same opponent on the same issues. In this case the relevant party is RAKIA but it has chosen not to appear or take any further part in these proceedings and it is not seeking to make the argument that the additional counterclaim would be an abuse. The Additional Defendants have taken up that mantle because they would obviously prefer not to have to deal with the additional counterclaim even though it will not really add to the evidential burden at the trial. Mr Masefield KC suggested that they may face an application in the future to be added as parties to the additional counterclaim and to face extra damages claims in relation to the recovery of the judgment sum awarded to RAKIA. However, I think there is little chance of that because the judgment sum has been paid into a secure account and can be returned to Mr Azima if he were to succeed in getting the First Judgment set aside.
104. I do think that some account has to be taken of the fact that it is the Additional Defendants, who are not parties to the proposed additional claim but who are the only ones opposing the grant of permission on the grounds of abuse of process. The oft-quoted passage from Lord Bingham's judgment in *Johnson v Gore Wood* [2002] 2 AC 1 (HL) at p.31 advocated a broad merits-based approach to abuse of process:

"That is to adopt too dogmatic an approach to what should in my opinion be a broad, merits-based judgment which takes account of the public and private interests involved and also takes account of all the facts of the case, focusing attention on the crucial question whether, in all the circumstances, a party is misusing or abusing the process of the court by seeking to raise before it the issue which could have been raised before."

105. Adopting that approach, the Additional Defendants are not and have not been sued in respect of this matter and they have to deal with the factual issues that arise anyway on the existing hacking counterclaim which has been remitted by the Court of Appeal. They can still say that because of the findings in the CA Judgment the Court should be astute to prevent its processes from being abused, and I will examine whether that is so, but if the impact on the Additional Defendants is limited, I think that is also a relevant factor that goes into the broad merits-based approach.

(b) Re-litigation

106. The Additional Defendants say that Mr Azima is seeking to run essentially the same case in the proposed additional counterclaim to that which he ran in the Court of Appeal. In the Court of Appeal he was arguing that, based on the new evidence then obtained (the phishing emails and Mr Rey's evidence), the Court of Appeal should find RAKIA responsible for the hacking and because that would necessarily have involved its witnesses giving dishonest evidence at the original trial, the whole trial process was "contaminated", including RAKIA's claims against Mr Azima. On the basis of Ground 5 of the appeal, Mr Azima was

asking the Court of Appeal to strike out RAKIA's claim or to exclude its evidence because the evidence had been obtained illegally. Alternatively, Mr Azima was asking that everything be retried, including RAKIA's claims and Mr Azima's hacking counterclaim so that the new Judge would be able to come to their own conclusions based on their own findings on the evidence and unbound by anything in the First Judgment. It is an important part of the Additional Defendants' case that Mr Azima had elected before the Court of Appeal to pursue his appeal and a remission to the High Court rather than bringing a fresh claim to set aside the First Judgment.

107. Mr Plewman KC disputed that the same issues were before the Court of Appeal. He submitted that the Court of Appeal was only considering the narrow issue raised by Ground 5, namely whether RAKIA's claim should be struck out or its evidence excluded on the *Summers v Fairclough Homes Ltd* and *Jones v University of Warwick* principles. The issue for the Court of Appeal was whether the deputy Judge was "wrong" whereas the issue in his proposed additional counterclaim is whether RAKIA's fraud was an operative cause of the deputy Judge's decision. Furthermore the fact that fraud had been raised before is no bar to bringing a claim to set aside the First Judgment if based on new evidence – see *Takhar* at [55] and [66]. And Mr Plewman KC said that there was substantial new evidence showing that there was pervasive dishonesty in RAKIA's pursuit of its claims against Mr Azima.

108. The Additional Defendants relied heavily on *Koshy v DEG-Deutsche Investitions-Und Entwicklungsgesellschaft mbh and anor* [2006] EWHC 17 (Ch), Rimer J (as he then was) (*Koshy*), and in the Court of Appeal at [2008] EWCA Civ 27 (*Koshy CA*). This was long-running litigation between the same parties, leading to a number of reported judgments. At the outset of the litigation there was a substantial costs order made by Harman J against Mr Koshy on 20 March 1998 in relation to Mr Koshy's failed application to discharge a freezing order. He did not appeal the order at the time but on 11 March 2002 was granted leave to appeal out of time on terms that he could only rely on two paragraphs of Rimer J's earlier judgment on the substantive issues. That appeal was ultimately dismissed. Then Mr Koshy tried to set off the costs ordered by Harman J against his liability to another party, but that failed. His third attempt to set aside the Harman J costs Order was to issue a fresh claim on 9 February 2005 to set aside the costs order on the grounds that it was procured by fraud. The defendants applied to strike out the claim mainly on the grounds of abuse of process and in particular because of an election made in the Court of Appeal to pursue the appeal rather than start fresh proceedings to set aside the order.

109. In *Koshy*, Rimer J struck out the new claim as an abuse of process because Mr Koshy had made an election to pursue the appeal and he should not be allowed to achieve the same outcome by using the different procedural route that he had previously decided against. At [66], Rimer J said:

"The Court of Appeal's view was that the just disposal of the issue that Mr Koshy's appeal had raised was either (i) the pursuit of the appeal, or (ii) a first instance trial of the factual questions it raised. But it was plainly of the view that both options should not be open to Mr Koshy and it gave him a choice as to which he wanted to pursue. If he chose the former, and failed, he was to understand that he could not re-open the matter in any other way, including (in my judgment) by a claim such as his new claim. Mr Koshy chose to pursue the appeal and must therefore be taken to have accepted that the price of doing so was the abandonment of all alternative procedural routes in the event of failure. He was therefore agreeing that he would not take any other procedural routes, and the Court of Appeal heard his appeal on that basis. In my view, in those circumstances the issue by Mr Koshy of his new 2005 claim was and is an abuse of the process of the court, since he was thereby taking a course which the Court of Appeal had made plain was not to be open to him and which he had agreed he would not take. I propose, therefore, to make an order striking the 2005 claim out".

110. The Court of Appeal in *Koshy CA* upheld Rimer J's decision, although it considered that he had not taken into account all the factors that he should have done as part of the "broad, merits-based judgment", in particular factors in Mr Koshy's favour such as the public interest in investigating claims that the court had been misled. However, Arden LJ (as she then was) gave the only judgment and she made clear that Mr Koshy had had a fair opportunity to pursue his case on the merits. At [33] – [34] she held:

"33. If Mr Koshy's allegations in the new action have substance, they clearly raise an important matter. Firstly, he alleges that a High Court judge was misled on a basic point that led the court into making an order for costs. In other words, he makes allegations about the integrity of the justice system and there cannot be any doubt but that it is of the utmost importance that the administration of justice should not be undermined by misinformation provided by one party ...

34. On the other hand, the issue is not now simply whether the allegations in the new action have substance but whether Mr Koshy has already had ample opportunity to have those allegations made the subject of judicial determination. Even though the allegations which Mr Koshy raises are of such seriousness and importance, nonetheless the justice system is not bound to provide more than one opportunity to run these issues. That is because the courts have to strike a fair balance between the interests of Mr Koshy on the one hand and of the other parties and the general interest on the other hand. That fair balance in my judgment is struck once Mr Koshy has had one effective opportunity to put his case."

111. Arden LJ went further still on the finality of litigation, holding that, even if Mr Koshy had not in fact had an opportunity to pursue an appeal on the merits, it was nonetheless an abuse of process to start a fresh action. After going through the factors in Mr Koshy's favour, she concluded at [58] and [59]:

"58. ...More fundamentally, Mr Koshy has already had at least one opportunity to have his claim fully ventilated in a court of law. He chose to have an adjudication of his claim on a limited basis ... Mr Koshy had been alerted to the potential difficulties in his appeal... There is a well-recognised public interest in the finality of litigation ...

59. ...For the reasons given, I would hold that it was an abuse of process for Mr Koshy to commence the new action and to seek to have another opportunity to bring a claim to have the order of Harman J as to costs set aside. In my judgment, the factors mentioned in the preceding paragraph, and in particular the factor that Mr Koshy has already had the opportunity to have an adjudication of the issues in the new action, which he rejected despite the clear warnings given by this court, outweigh the factors which weigh in his favour."

112. Mr Plewman KC submitted that *Koshy* was very different on the facts in particular as to whether there had been an explicit election to pursue one course over another and as to the new evidence available to the party seeking to bring the claim to set aside for fraud. Rimer J in [81] and [82] of *Koshy* had made it clear that Mr Koshy did not have any fresh evidence and he just wanted to re-run issues at a new trial that he could have run in the first trial based on the evidence available to him then. (This was confirmed by Arden LJ at [15] of *Koshy CA*.)

113. I think that the new evidence is a distinguishing feature to this case which is clearly based on the new evidence obtained since the CA Judgment, principally Mr Page's and Mr Halabi's affidavits, the Page invoices and the recently discovered Project Update Reports. This is significant new evidence, never considered before, and could be used to support an allegation of pervasive dishonesty practised on this Court by or on behalf of RAKIA.

114. But I also question whether the election point is properly levelled at Mr Azima. As explained above, Mr Lord KC's submissions to the Court of Appeal in relation to using the evidence to pursue the appeal or to start a fresh action were made during a discussion as to the appropriate procedural route for considering whether the whole of the First Judgment should stand or not. In other words, the contemplated fresh action was to set aside the First Judgment on the grounds that it had been procured by fraud. That included RAKIA's claims against Mr Azima. The discussion centred around Asplin LJ's judgment delivered the previous week in *Dale v Banga* which discussed the various options in this situation.

115. The issue in *Dale v Banga* was "what the appeal court should do when fresh evidence is adduced after a trial which allegedly shows that the judgment below was obtained by fraud, the conduct relied upon being

that of a witness and of a party to the action which took place after the events in issue, and is unrelated to the issues which were before the court": [1]. At [39] to [41], Asplin LJ explained the new practice after *Noble v Owens*:

"39. It is clear, therefore, that where an allegation of fraud is involved, there are two courses which may be adopted. The dissatisfied party may bring a new action to set aside the judgment already obtained on the basis that it was obtained by fraud: *Flower v Lloyd* [1877] 6 Ch D 297; *Hip Foong Hong v H Neotia & Company* [1918] QC 888; and *Jonesco v Beard* [1930] AC 298. Such a route was adopted in the *Royal Bank of Scotland* case and in the *Takhar* case. In such circumstances, the successful party retains the benefit of the judgment unless it is set aside and can seek to strike out the claim to set it aside as an abuse of the court's process.

40. In *Salekipour v Parmar* [2017] EWCA Civ 2141, [2018] QB 833, the Court of Appeal expressed a preference for this approach but did not decide the issue. The same preference was expressed by the Court of Appeal in *Daniel Terry v BCS Corporate Acceptances Limited, BCS Offshore Funding Limited, John Taylor* [2018] EWCA Civ 2442 at [38], although, once again, it was unnecessary to decide the point.

41. The second and alternative route, which is the one adopted here, is to appeal the original order, alleging that the judgment upon which it is based was obtained by fraud. A retrial will be ordered where the fraud is admitted or incontrovertible. Where, as in this case, it is neither admitted nor incontrovertible, a "*Noble v Owens* order" is sought by which the issue of fraud is remitted to the court below and decided within the same proceedings."

116. Again this is about setting the whole of the original judgment aside for fraud. That was the context for Mr Lord KC's submissions to the Court of Appeal. There was no discussion as to whether he would prefer a limited remission of just the hacking counterclaim or to be able to start a fresh action to set the First Judgment aside.
117. That is the cause of my confusion about the discussion at [135] to [146] of the CA Judgment. The Court of Appeal had already decided that RAKIA's judgment against Mr Azima would stand even if "*RAKIA was responsible for the hacking*": [122]. It then had to consider what to do with the hacking counterclaim – see [129]. It referred to the fresh evidence and then *Takhar* and *Dale v Banga*. It concluded that it would not be able to decide the factual question as to whether RAKIA was responsible for the hacking. The question was then posed whether it "*should remit the issue of fraud to the High Court within the existing proceedings; or leave Mr Azima to begin a fresh action.*"
118. I have referred above to it being unclear what that "*fresh action*" would be for and whether it would include setting aside the First Judgment in full. It is important to understand that because the Court of Appeal said that Mr Lord KC argued for remission of "*the issue of fraud*" whereas Mr Tomlinson KC wanted Mr Azima to start a fresh action. From my reading of the transcripts, that question was not actually put to and addressed by both Counsel. Both were arguing for one option rather than the other on the assumption that they included RAKIA's claims against Mr Azima. Mr Lord KC much preferred remission in those circumstances because RAKIA would not be able to raise objections to the jurisdiction of the Court. But the Court of Appeal transposed those arguments into the question that it was then considering as to how best to deal with the new evidence but solely in relation to the hacking counterclaim.
119. The Court of Appeal was only "*narrowly persuaded*" to go down the remission route. That means it was nearly persuaded that Mr Azima should have been allowed to begin a fresh action to set aside the judgment, although query whether that meant the whole of the First Judgment. But the Court of Appeal was absolutely clear that "*RAKIA's substantive claims stand*" whatever the findings on the remitted counterclaim.

120. What this means is that I do not accept that an election of the sort that was made by Mr Koshy was made by Mr Azima in the Court of Appeal. He did decide to pursue his appeal and he took it all the way to seeking permission from the Supreme Court. If he had no new evidence than was before the Court of Appeal, then he might have been in difficulties in arguing that he had not chosen how procedurally that evidence should be dealt with. But he made no unequivocal election that whatever new evidence might emerge in the future he would not seek to deploy it in a fresh action to set aside the First Judgment for fraud, assuming he could satisfy both the Fraud and Materiality Conditions.
121. The Additional Defendants also place heavy reliance on [40] of the CA Judgment where the Court of Appeal set out the factual assumptions it was making in Mr Azima's favour for the purposes of considering whether RAKIA's claims would in those circumstances have been struck out. They assert that Mr Azima's new evidence would only demonstrate that which the Court of Appeal assumed in his favour and so it could not have led to a different conclusion by the Court of Appeal.
122. However care needs to be taken in this respect to see what the Court of Appeal was assuming and whether that could be said to include the new evidence as to RAKIA's responsibility for the hacking and alleged perjury at the original trial. CA Judgment [40] is set out above: (b) was that "*RAKIA was responsible for that unlawful hacking*"; and (c) "*that at least some of RAKIA's witnesses gave dishonest evidence about how RAKIA came into possession of the hacked material*".
123. The assumptions set out at [40] of the CA Judgment do not, in my view, capture the scale and implications of the new evidence and what Mr Azima alleges it demonstrates. I do not think that the Court of Appeal could have had in contemplation there being evidence of an alleged "*perjury school*" taking place in a Swiss hotel shortly before the start of the original trial or the discovery of all the Project Update Reports that RAKIA had said had all been destroyed, save for the March 2015 one. The Court of Appeal was not assuming satisfaction of the Fraud Condition: "*conscious and deliberate dishonesty*"; rather it was merely assuming "*at least some of RAKIA's witnesses gave dishonest evidence*" and only in relation to the collateral issue of hacking. CA Judgment [61] refers to "*lies*" that Mr Page and Mr Halabi may have told, suggesting that the Court of Appeal was not assuming that RAKIA's most important witnesses, Mr Buchanan, Mr Gerrard and the Ruler, were giving dishonest evidence. And in its conclusions in this respect, the evidential assumption seems even weaker: "*even if the judge had found that RAKIA had been involved in the hacking of Mr Azima's email accounts*" [63]; "*even if RAKIA was responsible for the hacking*" [122]; and "*if the judge had found that RAKIA had been responsible for the hacking...*" [129]. There is no reference there to wholesale dishonesty by all of RAKIA's witnesses, potentially affecting their credibility on other issues.
124. Mr Plewman KC submitted that the assumptions were made by the Court of Appeal only for the purpose of considering whether to exclude RAKIA's evidence or to strike out its claims against Mr Azima. In other words, they were only to deal with what Mr Plewman KC said was his somewhat narrow Ground 5 of the appeal. However I think that this falls into the trap, as highlighted by Mr White KC, of relying on form over substance. Whether Mr Azima was seeking to have the judgment against him overturned by strike-out or the exclusion of evidence or to set it aside on the grounds of fraud should not affect the issues that I now have to decide.
125. Having said that, in my judgment, the proposed additional counterclaim would not amount to abusive re-litigation of issues and evidence that have been determined on the merits in the CA Judgment, or in the refusal of the Supreme Court to grant permission to appeal. Mr Azima made no unequivocal election that would preclude him from bringing a fresh action based on significant new evidence. Nor did the Court of Appeal contemplate that, whatever evidence may later emerge that might establish that a substantial fraud was perpetrated on the Court, Mr Azima should be debarred from bringing that evidence before the Court to try to prove that the First Judgment was procured by fraud.

(c) Collateral Attack

126. The Additional Defendants also rely on the collateral attack basis of abuse of process, the principles of which were articulated by the House of Lords in *Hunter v Chief Constable of the West Midlands Police* [1982] AC 529. They say that the proposed additional counterclaim would be a collateral attack on the CA Judgment and Order and also on the Supreme Court's refusal of permission to appeal. This was not pressed hard by Mr Masefield KC and it does seem to me that it adds little to the arguments that were run on re-litigation abuse, and my findings in such respect are similarly applicable.
127. Mr Masefield KC did point to the public policy reasons relied upon in the CA Judgment for not disturbing RAKIA's judgment against Mr Azima. These were:
- (1) The hacked documents "*ought to have been disclosed by Mr Azima anyway*" [62]; and they "*ought to have been available to RAKIA by the time of trial*" [47]; and
 - (2) The hacked documents "*revealed serious fraud on the part of Mr Azima which would have been a very serious bar to the grant of equitable relief in his favour*" [47]; and therefore "*to strike out RAKIA's claim would leave Mr Azima with the benefits of his fraud*" [62].
128. Mr Masefield KC said that those public policy reasons continue to apply notwithstanding the new evidence upon which Mr Azima seeks to rely. The Court of Appeal said that there were other ways for the Court to express its disapproval of a party using unlawful means to obtain evidence, such as in respect of interest and costs. The CA Order specifically provided in paragraph 12 that the only remedy available to the retrial Judge in respect of the judgment in RAKIA's favour that still stands would be in respect of interest and costs. However the Court of Appeal was careful to limit that to where the party has obtained "*evidence by unlawful means*" [62], leaving open perhaps the possible consequences if there was a more wide-reaching fraud established by new evidence.
129. It also seems to me that some care was taken in limiting the wording of the CA Order. Under paragraph 4, the declaration about the consequences of succeeding on the counterclaim was not put in those terms. Instead it referred to it being established that RAKIA "*was responsible for the hacking and dissemination of [Mr Azima's] data...*" suggesting that it was not precluding a more pervasive fraud being proved which may have different consequences.
130. I do not think that the collateral attack argument takes the matter beyond the points made above in relation to re-litigation and finality. In [117] of the CA Judgment, the Court of Appeal said, in a very different context, that it places "*considerable weight on the principle of finality*" and that was why it was not prepared to admit Mr Nayeibi's evidence on the unlawful conspiracy claim. But where the new evidence has not been tried and tested on its merits and where it potentially could lead to a finding that the Court was seriously deceived by coordinated perjured evidence, I do not see that the Court of Appeal was ruling out the possibility that Mr Azima could on that basis seek to set aside the First Judgment on the grounds of fraud. Indeed I do not think it would be right for it to do so when it has no idea what sort of new evidence might emerge.
131. Of course this is all dependent on the new evidence being significant enough to found such an action and I deal below with that point on the Materiality Condition. But assuming that it is, and adopting Lord Bingham's "*broad, merits-based judgment*" approach, it seems to me that in this case the "*fraud unravels all*" principle outweighs the finality principle, and it would not be an abuse of process for Mr Azima to bring either a fresh action or an additional counterclaim to set aside the First Judgment, the CA Judgment and their respective Orders.

THE MATERIALITY CONDITION

132. That leaves me to deal with the challenge of the Additional Defendants, principally through Mr White KC, to whether Mr Azima has a real prospect of establishing the Materiality Condition. I have already decided that the burden is on Mr Azima in respect of both Conditions and there is no dispute that at this stage he gets past the threshold on the Fraud Condition. I emphasise that I am not making any findings as to the

strength of the new evidence or whether Mr Azima is likely to be able to prove his allegations of fraud. I merely assume, for the purposes of considering this application and the low threshold test of real prospect of success, that those allegations can be established.

133. The overarching point that is made on behalf of Mr Azima is that if all of RAKIA's witnesses conspired together to give perjured evidence and to mislead the Court that would be bound to have affected their credibility generally including in relation to their evidence on RAKIA's fraudulent misrepresentation and conspiracy claims against Mr Azima. If that evidence had been available at the original trial it would have had a material effect and would at least have been "*an operative cause*".
134. In *Takhar 2*, Steven Gasztowicz QC referred to the "*melting pot of the evidence*" in relation to the Materiality Condition at [56]:

"If the relevant evidence (here the forged document) was something in the melting pot of the evidence before the court, whether relating directly to relevant facts or to relevant issues of credit, with all that is in the melting pot taken into account by it in coming to a judgment, whether or not one part is highlighted more than another, it will be "*an operative cause*."

135. Mr White KC criticised the notion of the "*melting pot of evidence*" and referred to the greater stringency that should be applied to the Materiality Condition where it is said to undermine the trial judge's general assessment as to a witness's credibility – this was the "*high hurdle*" that Burton J referred to in *Chodiev v Stein* at [23] and [45]. However in this case the alleged dishonest evidence was not purely as to credit; it was at the very least highly relevant to the hacking counterclaim. And I would respectfully endorse Leech J's dicta in *Tinkler* at [26]:

"there will be cases in which the new evidence is so fundamental to the credibility of the witness that it will be material even though it is not directly relevant to the substantive issues. For example, if a solicitor gives evidence that she is a solicitor and holds a valid practising certificate but conceals from the Court that she has been struck off for mortgage fraud, I would consider evidence of the striking off to be material. Likewise, where two witnesses conspire together to mislead the Court, I would consider evidence of the conspiracy to be material."

136. The deputy Judge seems to have agreed with that last sentence at [384] of the First Judgment, indicating that such new evidence would have had an operative effect:

"If, however, I had found that, as alleged by Mr Azima, not only had RAKIA hacked Mr Azima's emails and used them as the evidential basis of this case, but also that its witnesses had conspired to put forward a fabricated case concerning RAKIA's lack of involvement in the hacking, there would have been strong grounds to strike the proceedings out as an abuse of process, as envisaged in *Summers v Fairclough Homes Ltd.*"

137. Mr Plewman KC explained the particular respects in which the lack of credibility of RAKIA's witnesses as a result of the new evidence of their alleged fraud would have impacted on the deputy Judge's findings on RAKIA's claims.
138. In relation to the claims based on the Good Faith Representation:

(1) RAKIA's case was that Mr Buchanan had relied on Mr Azima's representation, and that the Ruler in turn had relied on Mr Buchanan's recommendation. Mr Buchanan had insisted in both his written and oral evidence that he had not believed that Mr Azima had engaged in any fraud or wrongdoing until the hacked data was released on the internet in August/September 2016, and that at the time of concluding the Settlement Agreement he was unaware of any evidence of wrongdoing. The deputy Judge found Mr Buchanan a generally reliable witness and that RAKIA had relied on the Good Faith Representation: [243.4] and [244].

(2) The deputy Judge also relied upon the Ruler's evidence that a purpose of the Settlement Agreement was *"to obtain assurance from [Mr Azima] that he had acted in good faith towards RAKIA and RAK more generally"*: [245].

(3) Mr Plewman KC submitted that the new evidence shows that RAKIA did not believe the Good Faith Representation and in fact believed Mr Azima had been engaged in persistent wrongdoing and fraud. Furthermore, if Mr Buchanan's and the Ruler's credibility was wrongly assessed in the light of the new evidence, the deputy Judge could not have found that RAKIA had relied on Mr Azima's representation.

(4) Further Mr Azima had contended that RAKIA did not rely upon the Good Faith Representation but included the good faith clause in the Settlement Agreement to *"trap"* him, so as to generate leverage over him in the wider battle between RAK and Dr Massaad - Mr Buchanan had said to the Ruler that the good faith clause was *"the key clause in this agreement bearing in mind your wider objectives"*: [311.3]. Although the deputy Judge found that there was some support for Mr Azima's submission, he ultimately rejected it for two reasons: he thought it was *"inherently unlikely"* that RAKIA would have paid Mr Azima \$2.6 million to enter into the Settlement Agreement if it had been hacking his emails by that stage: [312]; and he relied upon the evidence of Mr Buchanan and Mr Gerrard: [316]. The latter is covered by the credibility point. And the former could be undermined by the fresh evidence which Mr Plewman KC said makes plain that RAKIA was doing the very thing the deputy Judge held was *"inherently unlikely"*: they were already engaging in hacking and had the hacked material but, nevertheless, entered into the Settlement Agreement.

139. In respect of the Investment Representation, Mr Plewman KC submitted as follows:

(1) RAKIA's case was that it believed it had an obligation to compensate Mr Azima and HeavyLift for contributions to the joint venture, but that it had no information about the extent of the contribution. It therefore submitted that its entry into the Settlement Agreement was induced by HeavyLift's financial statements, which suggested that HeavyLift had spent a total of approximately \$2.6 million on its contribution to the Training Academy joint venture. The deputy Judge accepted that case on the basis of Mr Buchanan's evidence: [150] and an inference on the Ruler's position: [151]. That is therefore affected by the general credibility point.

(2) Mr Plewman KC submitted that the new evidence also shows that RAKIA could not have relied upon the Investment Representation, because it:

- (a) Suggests RAKIA did not believe it had any obligation to compensate HeavyLift;
- (b) Shows that RAKIA's own investigators told RAKIA that information was being withheld from RAKIA in its negotiations over HeavyLift's claim: see the "Project Beech – Update Report" dated 17 August 2015; and
- (c) Demonstrates that RAKIA was already aware of at least some of the very documents which it submitted at trial showed the Investment Representation to be false.

140. Mr Plewman KC submitted that RAKIA's alleged fraud also undermined the rejection of Mr Azima's and Mr Adams' evidence in relation to the misrepresentation claims. He said that the new evidence shows that Mr Azima and Mr Adams were giving accurate evidence about critical contested issues.

141. As to the unlawful conspiracy claim, Mr Plewman KC said that:

(1) The foundation of the claim was RAKIA's allegation that Mr Azima did not introduce the potential buyers of the Hotel to RAKIA Georgia. If he did introduce them, the payment of a commission would be both logical and commercially sound.

(2) Mr Azima's evidence was that the Ruler knew and approved of the payment of commission and RAKIA provided no documentary evidence as to how the transaction unfolded, claiming it had no documents.

(3) The deputy Judge ultimately concluded that Mr Azima had not introduced the buyers on the basis of the Adams Memorandum which had been prepared more than four years after the events in question: [176]. He rejected Mr Adams' and Mr Azima's evidence that the reference to being introduced to the buyers during the negotiations was a mistake: [176]-[177] and (by implication) accepted the Ruler's evidence that he had not approved the commission: [181]. In consequence he concluded that the referral agreement was a sham: [181.3] and [181.6]; which in turn was a material basis for the further finding that a payment by Mr Azima to Dr Massaad was a bribe (an inference drawn from the absence of any entitlement by Mr Azima to payment): [186].

(4) The general credibility argument applies and means that no reliance could be placed on the Ruler's denial that he knew and approved of the payment and the deputy Judge would have been bound to accept Mr Azima's case.

142. On the basis of the above, it is difficult to see how it could be argued that Mr Azima has no real prospect of satisfying the Materiality Condition, assuming that he can prove the pervasive fraud on the Court that he alleges. It would be open to the Additional Defendants to challenge the materiality of the new evidence at trial, but at this stage they would have to show that his case is fanciful and could not succeed.

143. Mr White KC attempted to do so by reference in particular to the assumptions in Mr Azima's favour made by the Court of Appeal in [40] of the CA Judgment. He said that Mr Azima must show that the new evidence goes well beyond the assumptions that the Court of Appeal made otherwise Mr Azima cannot submit that it would have impacted the conclusions in the CA Judgment.

144. Mr White KC referred to the way Mr Azima proposed pleading the fresh evidence in the draft RRRACC, in particular Schedule B, and framed his submissions around five categories of allegedly fraudulent evidence which Mr Azima relies upon to justify setting aside the First Judgment and the CA Judgment. Those categories were as follows:

(1) evidence that the witness lacked knowledge of the hacking of, and/or illegal access to, Mr Azima's data;

(2) evidence that the witness lacked knowledge of wrongdoing by Mr Azima prior to September 2016;

(3) evidence as to RAKIA's objectives in entering into the Settlement Agreement with Mr Azima/the denial that the Settlement Agreement was a "trap";

(4) evidence denying that investigations were conducted into Mr Azima, and/or that Mr Azima was considered one of Dr Massaad's "associates", prior to September 2016; and

(5) evidence as to RAKIA's lack of knowledge, and/or RAKIA's concealment of evidence, that Mr Azima had introduced the purchasers of the Hotel.

145. Mr White KC's submission, as I understand it, was that categories (1), (2) and (4) are all implicitly covered by the assumptions in [40] of the CA Judgment and therefore were taken into account by the Court of Appeal in concluding that they could not affect RAKIA's judgment against Mr Azima. As to category (3), Mr White KC said that there was simply no evidence in the new material that this was RAKIA's objective. And category (5) could not impact the First Judgment or the CA Judgment because the main reason for the decision on the conspiracy claim was that a "bribe" was paid by Mr Azima to Dr Massaad.

146. I repeat what I said in [123] above as to whether the assumptions made by the Court of Appeal really do capture the full extent of Mr Azima's allegations of "pervasive dishonesty" in respect of RAKIA's evidence

at the original trial. Mr Azima makes direct allegations about Mr Buchanan's, Mr Gerrard's and the Ruler's participation in that dishonesty and conspiracy to deceive the Court and the effect on their credibility generally. The Court of Appeal assumed only that "*at least some of RAKIA's witnesses gave dishonest evidence*" and, at [61], perhaps indicated that this was limited to Mr Page and Mr Halabi and only to "*lies*" given on the collateral issue of hacking, not on RAKIA's substantive claims. I cannot be sure that the Court of Appeal was assuming that there was "*pervasive dishonesty*" amongst all of RAKIA's witnesses, including those whose evidence was relied on by the deputy Judge in coming to his decision on RAKIA's claims against Mr Azima.

147. Accordingly I do not think it is right to frame considerations of the Materiality Condition around the assumptions made by the Court of Appeal. I have to decide whether Mr Azima has a real prospect of showing that the alleged fraud and conspiracy between RAKIA's main witnesses to mislead the Court is material. In my view he has plainly crossed that low threshold.

CONCLUSION

148. For the reasons set out above, I reject the Additional Defendants' arguments on jurisdiction and abuse of process and consider that Mr Azima has a real prospect of succeeding in his proposed new additional counterclaim to set aside the First Judgment, the CA Judgment and their respective Orders on the ground that they have been procured by fraud. Accordingly I grant permission to Mr Azima under CPR 20.4(2)(b) to bring the additional counterclaim against RAKIA.

149. As noted above, it was agreed that Mr Azima's application under CPR 17.1(2)(b) to make amendments to his existing counterclaim would be held over to be dealt with after delivery of this judgment. If those amendments cannot be agreed a further hearing will have to be arranged. Similarly there are other consequential matters, such as directions as to the timing of disclosure and other events, as well as costs which will have to be dealt with at some point and I leave it to the parties to arrange a hearing should that be necessary.

BAILII: [Copyright Policy](#) | [Disclaimers](#) | [Privacy Policy](#) | [Feedback](#) | [Donate to BAILII](#)

URL: <http://www.bailii.org/ew/cases/EWHC/Ch/2022/2727.html>

EXHIBIT 42

Judgments in favour of Emirati sovereign wealth fund set aside on grounds of fraud by the fund

26/03/24

The High Court has granted default judgment setting aside two High Court judgments and one Court of Appeal judgment, on the grounds that they were procured by fraud. This brings to an end a very long-running saga.

The Ras Al Khaimah Investment Authority, RAKIA, is the sovereign wealth fund for Ras Al Khaimah, one of the seven of the United Arab Emirates. In September 2016, it sued Mr Farhad Azima, an American businessman, alleging that he had defrauded it and conspired with its former CEO and others to obtain commission payments. RAKIA relied on various documents forming part of some 30GB of data hacked from Mr Azima's emails and computers and placed online on anonymously hosted websites.

Mr Azima denied the claims, alleged that RAKIA had been responsible for the hacking and counterclaimed. RAKIA strenuously denied any involvement in the hacking or knowledge of how it occurred. Following a trial in January-February 2020, Mr Andrew Lenon KC (sitting as a Deputy High Court Judge) largely upheld RAKIA's claims, awarding damages, costs and interest; found that Mr Azima had not proved that RAKIA was responsible for the hacking and dismissed Mr Azima's counterclaim. (See news item, [here](#))

In March 2021, the Court of Appeal (Lewison, Asplin and Males LJ) remitted the counterclaim for retrial but otherwise rejected Mr Azima's appeal, and directed that in any remitted trial, the Deputy Judge's findings against Mr Azima "must stand". (See news item, [here](#)).

The remitted counterclaim was assigned to Mr Justice Michael Green. Mr Azima was granted permission to add additional defendants: Mr Neil Gerrard (then a partner in the law firm Dechert), Dechert, Mr James Buchanan (an executive who had managed RAKIA's activities) and an investigator, Mr Stuart Page.

As the counterclaim progressed, Mr Azima obtained a range of new evidence, including hundreds of pages of reports prepared for RAKIA, which contained masses of Mr Azima's private and confidential data, long before any of his data had been placed online. Mr Page provided an affidavit admitting that his evidence at the first trial had been concocted and the claim against him was discontinued.

In June 2022, Mr Azima applied for permission to bring an additional counterclaim, alleging that RAKIA was complicit in the hacking and had falsely denied this, but also that (in view of the new evidence), the judgment on RAKIA's own claims had been procured by RAKIA's fraud (the 'Set Aside Counterclaim').

Very shortly before that application was made, RAKIA advised the Court that it was withdrawing its instructions to its solicitors, that it was not providing a new address for service, and that it would not participate further in the proceedings.

The additional defendants (Mr Gerrard, Mr Buchanan and Dechert) opposed Mr Azima bringing the Set Aside Counterclaim, alleging that it constituted an abuse of process in view of the Court of Appeal's ruling that the Deputy Judge's findings on RAKIA's claims "must stand", and that the fraud alleged against RAKIA was not sufficiently material so as to undermine the Deputy Judge's findings on RAKIA's claims. Mr Justice Michael Green rejected those arguments and granted permission to bring the Set Aside Counterclaim. This decision was upheld by the Court of Appeal (see news items [here](#) and [here](#)).

The two counterclaims were listed for a trial to commence in May 2024.

Mr Azima then applied for default judgment against RAKIA in respect of both his original hacking counterclaim and the Set Aside Counterclaim. Mr Justice Michael Green granted the former application, but refused the latter on the ground that the additional defendants might be prejudiced if default judgment were granted. (see news item [here](#))

In January 2024 Mr Azima accepted a Part 36 offer made by Dechert and Mr Gerrard, and in March 2024 he concluded a confidential settlement with Mr Buchanan. This brought to an end the proceedings against the additional defendants. He then brought a renewed application for default judgment against RAKIA on the Set Aside Counterclaim, and an application for his remedies on the hacking counterclaim.

The Judge granted default judgment on the Set Aside Counterclaim, observing that RAKIA's conduct was, "*an egregious case*", that "*has had the somewhat extraordinary consequence that they obtained judgments by fraud from both first instance and the Court of Appeal*".

The Judge also assessed Mr Azima's remedies against RAKIA under the hacking counterclaim, awarding £200,000 for non-pecuniary damage for emotional distress, £100,000 in exemplary damages and injunctive relief against RAKIA; and awarded Mr Azima his costs of the earlier proceedings and the Set Aside Counterclaim on the indemnity basis.

The Judge's Order is [here](#).

Thomas Plewman KC, Hugo Leith, and Frederick Wilmot-Smith (instructed by Burlingtons Legal LLP) appeared for Mr Azima on the renewed application for default judgment.

Tim Lord KC and Sophie Bird acted for Mr Azima at earlier stages of the proceedings.

Fionn Pilbrow KC and Aarushi Sahore acted for Mr Gerrard at earlier stages of the proceedings.